

#2

Attorney Docket No. 1341.1108

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Satoru TORII, et al.

Application No.:

Group Art Unit:

Filed: September 20, 2001

Examiner:

For: METHOD OF AND SYSTEM FOR MANAGING INFORMATION, AND COMPUTER
PRODUCT

11036 U.S. PTO
09/955972
09/20/01

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith
a certified copy of the following foreign application:

Japanese Patent Application No. 2000-387880

Filed: December 20, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 20, 2001

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1036 U.S. PTO
09/955972
09/20/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: 2000年12月20日

出 願 番 号
Application Number: 特願2000-387880

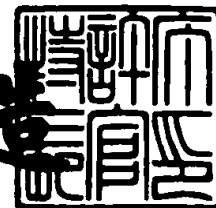
出 願 人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 6月 4日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



Best Available Copy

出証番号 出証特2001-3052493

【書類名】 特許願

【整理番号】 0051969

【提出日】 平成12年12月20日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 3/00

【発明の名称】 情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 鳥居 悟

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 三友 仁史

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 滝沢 文恵

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 通信要求を監視する通信要求監視手段と、前記通信要求監視手段から通知された情報に基づいて対策を選択する管理手段と、前記管理手段からの指示に応答して対策を実施する実施手段とを有し、

前記管理手段は、

前記通信要求監視手段からの通知内容と前記実施手段が実施する対策とを対応づけて管理するデータベースと、

前記データベースに基づいて対策を選択する選択手段と、

を備えたことを特徴とする情報管理システム。

【請求項 2】 攻撃事象若しくは漏洩事象の進行過程における 2 以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集手段と、前記情報収集手段により収集整理された情報を前記データベースに反映する反映手段と、をさらに備えたことを特徴とする請求項 1 に記載の情報管理システム。

【請求項 3】 前記選択手段は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする請求項 1 または 2 に記載の情報管理システム。

【請求項 4】 前記データベースは、前記通信要求監視手段により通知される情報を時系列で保持し、前記選択手段は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする請求項 1、2 または 3 に記載の情報管理システム。

【請求項 5】 前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成手段をさらに備えたことを特徴とする請求項 1 ～ 4 のいずれか一つに記載の情報管理システム。

【請求項 6】 システムの脆弱性を示す脆弱性呈示手段と、前記脆弱性呈示手段に対する攻撃に関する情報を収集する情報収集手段と、をさらに備えたこと

を特徴とする請求項 1 ～ 5 のいずれか一つに記載の情報管理システム。

【請求項 7】 通信内容の発信元を調査する調査手段と、前記調査手段による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定手段と、をさらに備えたことを特徴とする請求項 1 ～ 6 のいずれか一つに記載の情報管理システム。

【請求項 8】 攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに備えたことを特徴とする請求項 1 ～ 7 のいずれか一つに記載の情報管理システム。

【請求項 9】 通信要求を監視部によって監視する通信要求監視工程と、前記通信要求監視工程により通知される通知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、を含んだことを特徴とする情報管理方法。

【請求項 1 0】 通信要求を監視部によって監視する通信要求監視工程と、前記通信要求監視工程により通知される通知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

この発明は、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる情報管理システム、情報管理方法および記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

近年のネットワーク技術の進展に伴って、インターネット上の分散システムである WWW (World Wide Web) の利用が急速に拡大し、情報を提供する各種 H T

TPサーバも累増してきたが、かかるサーバの増加とともに不正アクセスも増加しつつある。

【0003】

この不正アクセスには、ネットワーク上のセキュリティホールを探知し、このセキュリティホールを介してシステムに侵入攻撃するものが知られており、この場合には、（１）稼働ホストを探知し、（２）提供サービスを探知し、（３）ネットワーク構成を探知し、（４）OSを識別し、（５）アプリケーションを識別し、（６）セキュリティホールを探知するという手順でセキュリティホールが探知される。そして、複数の踏み台サイトを使用してターゲットに対して大量のパケットを送り込むなどしてシステムエラーを導き、その後不正アクセスがなされることになる。

【0004】

ここで、この不正アクセスは、一般的なアクセスと明確に区別することができないため、通常は進入攻撃がおこなわれるまでシステム管理者が不正アクセスを検知することが難しいという特性がある。

【0005】

このため、従来は、サイトに対して送り込まれる大量のパケットを認識した際に、できる限り迅速に不正アクセスによる実被害を極小化する対策が採られるのが一般的である。

【0006】

【発明が解決しようとする課題】

しかしながら、ターゲットとなるサイトに一旦攻撃が開始されると、この攻撃を防御することは極めて難しく、また理想的な対策を講じたとしても、一時的にサイトを閉鎖せざるを得ないという問題が生ずる。特に、銀行や交通機関のように多数のユーザに対して継続的にサービスを提供するサイトでは、一時的にサイトを閉鎖することによる影響が各方面に波及し、膨大な実被害をもたらす可能性もある。

【0007】

このため、かかる不正アクセスによる被害をいかに極小化するかが極めて重要

な課題となっており、望ましくは、不正アクセスがなされたとしても全く被害が生じない枠組みが必要とされている。

【 0 0 0 8 】

この発明は、上述した従来技術による課題を解消するためになされたものであり、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項 1、9 および 10 の発明によれば、図 2 に示すデータベース 201 内に通知内容 (A) と対策 (B) を対応づけて保持しておき、モニタエージェント 203 (通信要求監視手段) が通信要求を監視して異常を検知して管理マネージャ 202 (管理手段) に通知すると、この管理マネージャ 202 (管理手段) が、データベース 201 から対策を選択して、アクションエージェント 204 (実施手段) に対策を実行させることとしたので、対策を効率良く実行することができ、もって、実際の攻撃に適切な対策を施して被害の極小化を図ることができる。

【 0 0 1 0 】

また、請求項 2 の発明によれば、攻撃事象若しくは漏洩事象の進行過程における 2 以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベースに反映することとしたので、データベースの内容を充実させ、より適切な対策を選択することができる。

【 0 0 1 1 】

また、請求項 3 の発明によれば、データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することとしたので、データベースのみならずシステムを取り巻く環境を考慮した上で妥当な対策を選択することができる。

【 0 0 1 2 】

また、請求項 4 の発明によれば、データベースが通信要求監視手段により通知される情報を時系列で保持し、このデータベースに記憶した時系列の情報に基づいて対策を選択することとしたので、時系列的な情報を用いて対策を選択することができる。

【 0 0 1 3 】

また、請求項 5 の発明によれば、複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成することとしたので、空間的な情報を用いて対策を選択することができる。

【 0 0 1 4 】

また、請求項 6 の発明によれば、システムの脆弱性を明示的に呈示し、この脆弱箇所に対する攻撃に関する情報を収集することとしたので、悪意者による攻撃手法を把握することができる。

【 0 0 1 5 】

また、請求項 7 の発明によれば、通信内容の発信元を調査した調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定することとしたので、踏み台とされているサイトを効率良く特定することができる。

【 0 0 1 6 】

また、請求項 8 の発明によれば、攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、この攻撃対象サイトへの攻撃を回避させるおとりサイトを設けることとしたので、攻撃対象サイトの保全を図るとともに攻撃手法を把握することができる。

【 0 0 1 7 】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係る情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【 0 0 1 8 】

まず、本実施の形態に係る全体システムに採用した各種技術について説明する。図 1 は、本実施の形態に係る全体システムに採用した各種技術を説明するため

の説明図である。同図に示すように、このシステムでは、誘導／情報収集技術、データベース化技術、予知技術、信頼性回避技術および攻撃回避技術などを駆使している。

【0019】

具体的には、この誘導／情報収集技術は、脆弱性を表に出して攻撃者（悪玉ハッカー）101による攻撃をおとりサーバ102に誘導するものであり、アンダーグラウンド情報、被害サイト情報並びに誘導して起こした攻撃によって攻撃に関する情報を収集し、得られた情報を解析して攻撃パターンとして認識する。

【0020】

また、データベース化技術は、解析した攻撃パターン、被害予想、対策案をデータベース化するものであり、たとえば、図中に示したUG系サイト群（善玉ハッカー）103、おとりサーバ102および被害サーバ104に対するアクセス手法とその対策を事例データベース105に蓄積する。

【0021】

また、予知技術は、事例データベース105を用いて、現時点で起こっている状況から攻撃の予兆を検知し、これにより起こり得る攻撃を予知するものであり、具体的には、攻撃者101による現時点での状況をパケットモニタ群106で検知する。

【0022】

また、攻撃回避技術は、事例データベース105を用いて、攻撃の進捗、環境などの情報から現時点で最適な回避対策を選択するものであり、たとえば図中の踏み台群107を踏み台とする防御対象サーバ108への攻撃をおとりサーバ109に誘導して攻撃を回避する。また、信頼性検知技術は、攻撃元と思われるサイトに対して、たとえば踏み台になっていないかなどの検査をおこなうものである。

【0023】

次に、図1に示した予知技術についてさらに詳細に説明する。この予知技術は、現実の攻撃あるいは誘導して起こした攻撃において、そのパターンの解析から、単発だけではなく、複数の種々の事象を空間的／時間的に連携づけた形で攻撃

を起こす予兆をデータベース化し、その予兆に対する攻撃の影響範囲、影響度合い、被害レベルを関連づけた形で整備し、半自動的にアップデートする。

【0024】

また、単発だけではなく、複数の種々の事象を関連づけた形で認識し、事例データベース105に照らし合わせて、予兆あるいは予兆候補として検知する。そして、検知した予兆および予兆候補を自ら解釈するだけではなく、下流サイトなどの他サイトへ通知する。

【0025】

さらに、自ら検知したサイトまたはたとえば上流サイトから通知された予兆および予兆候補から、事例データベース105に照らし合わせて、将来起こり得る攻撃を予知する。この攻撃の予知は、事例データベース105の情報にしたがって、影響範囲、影響度合い、被害レベルなどについておこなう。

【0026】

このように、かかる予知技術は、(1)不正アクセス手法とその予兆現象のデータベース化、(2)予兆検知、(3)予兆／予兆候補通知、(4)攻撃予兆などからなる。

【0027】

(1)不正アクセス手法とその予兆現象のデータベース化

アンダーグラウンド(UG)系サイト群103で公開される不正アクセス手法を収集および解析し、被害サーバ104(他サイト)で実際に発生した攻撃手法を収集および解析し、おとりサーバ102によって脆弱性を表に出して攻撃を誘導し、その攻撃手法を収集および解析する。

【0028】

そして、これらの解析結果をもとに、単発だけではなく複数の種々の事象を空間的／時間的に連携づけた形で攻撃パターンの解析をおこない、攻撃を起こす予兆をデータベース化する。その予兆に対する攻撃の影響範囲、影響度合い、被害レベルを関連づけた形で整備し、事例データベース105を半自動的にアップデートする。

【0029】

(2) 予兆検知

特定サイトへ向けた定常状態とは異なるパケット到着状態を検出し、また特定サイトでの定常状態と異なるパケット到着状態を検出し、これらの検出結果をもとに、単発だけではなく複数の種々の事象を連携づけた形で認識し、この認識結果をもとに、事例データベース 1 0 5 の内容と照らし合わせて、予兆または予兆候補を検知する。

【 0 0 3 0 】

(3) 予兆／予兆候補通知

検出した予兆および予兆候補をたとえば下流サイトのような他サイトに通知する。たとえば、特定サイトへ向けた定常状態とは異なるパケット発信を依頼された際には、そのパケットを送信するとともに、「このパケットは〇〇攻撃の予兆である可能性がある」という情報を、そのサイトに通知する。

【 0 0 3 1 】

(4) 攻撃予兆

自ら検知し、また上流サイトのような他サイトから通知された予兆および予兆候補を事例データベース 1 0 5 の内容と照らし合わせることで、将来起こり得る攻撃を予知する。

【 0 0 3 2 】

次に、図 1 に示した攻撃回避技術についてさらに詳細に説明する。この攻撃回避技術は、攻撃を受けた履歴から、攻撃の進捗過程のそれぞれにおける回避手段を攻撃対象の種別、環境条件ごとに考察し、その回避手段を、予兆／攻撃と関連づける形でデータベース化し、半自動的にアップデートする。

【 0 0 3 3 】

そして、攻撃を予知した後に、現時点が予知された攻撃のどの段階にあるのかを予測し、攻撃対象、環境条件を見だし、事例データベース 1 0 5 から最適の回避手段を決定する。その後、決定した回避手段を行使して、攻撃を未然に防止する。したがって、かかる攻撃回避技術は、(1) 回避手段のデータベース化、(2) 回避手段の選択、(3) 回避手段の行使などからなる。

【 0 0 3 4 】

(1) 回避手段のデータベース化

攻撃を受けた履歴から、攻撃の進捗過程のそれぞれにおける回避手段を、攻撃対象の種別、環境条件ごとに考察、開発および検証し、その回避手段を予兆／攻撃と関連づける形でデータベース化し、半自動的にアップデートする。

【0035】

(2) 回避手段の選択

攻撃を予知した後、現時点が予知された攻撃のどの段階にあるかを予測する。そして、予知した攻撃の対象を見極め、環境条件を見いだす。そして、攻撃の進捗具合、攻撃対象、環境条件を事例データベース105と照らし合わせて最適の回避手段を決定する。

【0036】

(3) 回避手段の行使

攻撃を予知する材料となった予兆／予兆候補を通知した上流サイトに対して通知し、その予兆／予兆候補のもととなったパケット発信元の信頼性検査を促す。また、攻撃の被害の拡大を防ぐため、破棄すべきパケットを選定してこれを破棄する。さらに、攻撃の被害の拡大を防ぐため、破棄すべきパケットを選定し、そのパケットを発信する可能性がある上流サイトに対して発信をしないように促す。また、攻撃を受けつつあることを他のサイトに通知して、同様の攻撃が他のサイトにおこなわれないう促す。さらに、攻撃を検知したサイトを模したおとりサーバ109を設け、それ以降の攻撃をおとりサーバ109側へと導く。

【0037】

ここで、このおとりサーバ102および109について具体的に説明する。かかるおとりサーバ102および109は、脆弱性があるふりをして攻撃を誘うサーバであり、(1) ユーザ名の変更(管理者権限)、(2) ログインメッセージ(OSや版数)の変更、(3) アプリケーション名や版数の変更、(4) 稼働ネットワークの偽称、(5) 脆弱なCGIプログラムの存在を偽称などを通じて、脆弱性があるふりをする。

【0038】

(1) ユーザ名の変更(管理者権限)

たとえば、ウィンドウズにおいて、初期設定時には管理者権限を持つユーザは「Administrator」であるが、新規にユーザ「Kanrisya」を設定して管理者権限を持たせ、従来のユーザ「Administrator」から管理者権限を外すことにより、システムが脆弱であるかの如く思わせることができる。

【 0 0 3 9 】

(2) ログインメッセージ (OS や版数) の変更

通常のSolarisマシンにおけるログインメッセージは、下記のようなになる。

```
SunOS 5.6
login:user-name
Password:*****
last login: Tue Aug 29 08:52:55 on console
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
%
```

【 0 0 4 0 】

ここで、以下のように表示するようにログインメッセージを変更し、現実とは別の (古いシステムで過去の脆弱性が残っている) OS が稼働しているように見せることにより、システムが脆弱であるかの如く思わせることができる。

```
TurboLinux release 3.2(***)
Kernel 1.2.9 on an i386(host.domain.company.co.jp)
login:user-name
Password:*****
%
```

【 0 0 4 1 】

(3) アプリケーション名や版数の変更

ウェブサーバに対して、HEADメッセージを送付すると、以下のようにサーバアプリケーション名を返す。

```
HTTP/1.1 200 OK
Data:Sat,1 Jan 2000 10:25:12 GMT
Server:Apache/1.3.9(Unix)
```

【 0 0 4 2 】

ここで、以下のように返答メッセージを変更し、現実とは別のアプリケーション（古いシステムで過去の脆弱性が残っているもの）が稼働しているように見せることにより、システムが脆弱であるかの如く思わせることができる。

HTTP/1.0 200 OK

Server:Microsoft-IIS/3.0

Date:Sat,01 Jan 2000 10:25:25 GMT

【 0 0 4 3 】

（４）稼働ネットワークの偽称

ポートスキャンなどの悪用ツールを用いることで、稼働中のネットワークサービスを調査することができる。

Port	State	Protocol	Service
21	open	tcp	ftp
80	open	tcp	www-http
443	open	tcp	https

【 0 0 4 4 】

ここで、虚偽の「ネットワークサービス受付機構」を用意し、その虚偽サービス（脆弱なサービス、port 23,79,110,111,143）へのアクセスをすべて監視するようにする。その結果として、ポートスキャンなどの悪用ツールにより、以下のような（虚偽の）調査結果が得られ、脆弱なサービスが稼働しているように誤認させることができる。

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
79	open	tcp	finger
80	open	tcp	www-http
110	open	tcp	pop3
111	open	tcp	sunrpc
143	open	tcp	imap

443 open tcp https

【 0 0 4 5 】

(5) 脆弱なCGIプログラムの存在を偽称

スキャンツールなどの悪用ツールを用いることで、提供可能なCGIプログラムの存在が検査できる。

Searching for _vti_inf.html : [Not Found]

Searching for service.pwd : [Not Found]

Searching for users.pwd : [Not Found]

Searching for authors.pwd : [Not Found]

Searching for administrators : [Not Found]

Searching for shtml.dll : [Not Found]

Searching for shtml.exe : [Not Found]

...

Searching for [perl.exe] . : [Not Found]

Searching for [wwwboard.pl] : [Not Found]

Searching for [www-sql] . : [Not Found]

【 0 0 4 6 】

ここで、脆弱性の存在が知られている既知のCGIプログラム（と同一名のファイル）を用意しておく。

% touch cgi-bin/phf cgi-bin/Count cgi-bin/test-cgi cgi-bin/phf.cgi

% touch cgi-bin/webgais cgi-bin/perl.exe cgi-bin/www-sql

% touch _vti_inf.html

% mkdir _vti_bin _inf.html _vti_pvt cfdocs

% touch _vti_bin/shtml.exe _vti_pvt/service.pwd _vti_pvt/authors.pwd

% touch cfdocs/zero.cfm cfdos/root.cfm

【 0 0 4 7 】

結果として、スキャンツールなどの悪用ツールにより、以下のような（虚偽の）調査結果が得られ、脆弱なCGIプログラムが存在しているように認識させることができる。

```

Searching for _vti_inf.html      : [Found!]
Searching for service.pwd       : [Found!]
Searching for users.pwd         : [Not Found]
Searching for authors.pwd       : [Found!]
Searching for administrators    : [Not Found]
Searching for shtml.dll         : [Not Found]
Searching for shtml.exe         : [Found!]
...
Searching for [perl.exe ].      : [Found!]
Searching for [wwwboard.pl]     : [Not Found]
Searching for [www-sql].        : [Found!]

```

【 0 0 4 8 】

次に、本実施の形態に係る情報管理システムの基本構成などについて図 2 ～図 1 3 を用いて説明する。図 2 は、本実施の形態に係る情報管理システムの基本構成を示すブロック図である。同図に示すように、この情報管理システムは、データベース（DB）2 0 1 を有する管理マネージャ 2 0 2 と、モニタエージェント 2 0 3 と、アクションエージェント 2 0 4 とからなる。

【 0 0 4 9 】

このデータベース 2 0 1 には、データ A と対策 B が対応づけて蓄積されており、管理マネージャ 2 0 2 は、モニタエージェント 2 0 3 からデータ A の通知を受け付けたならば、データベース 2 0 1 の内容を参照して対策 B および対策の依頼先（アクションエージェント 2 0 4 ）を特定し、このアクションエージェント 2 0 4 に対して対策 B の実行を指示する。また、攻撃事象若しくは漏洩事象の進行過程における 2 以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベース 2 0 1 に反映する。

【 0 0 5 0 】

具体的には、モニタエージェント 2 0 3 が、ファイアウォールや WWW サーバ（以下、「エンティティ」と言う）のログを分析して異常を検知したならば、異常が発生した旨を示すデータ A を管理マネージャ 2 0 2 に通知する。そして、管

理マネージャ202は、データベース201を参照して対策Bを特定する。具体的には、このデータベース201は、モニタエージェント203から通知されたデータを時系列で保持し、この時系列のデータに基づいて管理マネージャ202が対策Bを選択する。

【0051】

たとえば、この対策Bとしては、「WWWサーバに異常が発生した場合に、ファイアウォールやWWWサーバへの通信を通さないようにする」という対策などがある。なお、図3に示すように、かかるモニタエージェント203およびアクションエージェント204は、複数存在しても良い。

【0052】

ここで、上記モニタエージェント203は、データAを取得した際に該データAそのものを管理マネージャ202に通知することとしたが、図4に示すように、管理マネージャ202が、重み付けしたデータAと重み付けした対策Bを対応づけて保持することもできる。

【0053】

図5は、かかる場合におけるモニタエージェント203の構成を示すブロック図である。同図に示すように、モニタエージェント203は、データ解析部203a、データ分析部203b、データスタック203c、重みテーブル203d、判定処理部203eおよび通知部203fからなる。

【0054】

すなわち、このモニタエージェント203は、データ解析部203aによりデータAをデータ解析し、データ分析部203bによりそのデータを分析して、データスタック203cに蓄積する。このデータスタック203cに蓄積されるデータは、時系列ごとに保持される。そして、あらかじめ準備した重みテーブル203dに基づいて、判定処理部203eが重みを判定し、通知部203fが重み付きの事象Aを管理マネージャ202に通知する。なお、かかる重み付けに用いる重み係数は、ユーザが任意に設定することができ、また、実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定することもできる。

【0055】

次に、図2に示した管理マネージャ202について説明する。図6は、図2に示した管理マネージャ202を説明するための説明図である。同図に示すように、この管理マネージャ202は、すでに説明したように、モニタエージェント203からデータAを受け付けた際に、データベース201を参照して対策Bを特定することになるが、この際、システム構成205および運用状況206などについても考慮する。

【0056】

また、この管理マネージャ202では、図7に示すように、各モジュール207からサイトに関する空間情報を取得し、取得した空間情報に基づいてサイトの物理マップ（サイトマップ）208を作成する。なお、ここで言うモジュール207には、各種モニタエージェント203およびアクションエージェント204が含まれる。

【0057】

また、図8に示すように、この管理マネージャ202は、モニタエージェント203に対してフィードバックをおこなっており、具体的には、管理マネージャ202は、モニタエージェント203のデータ分析部203bで使用する分析ルールをモニタエージェント203に対して配布する。このように、管理マネージャ202の主導のもとに、モニタエージェント203の分析ルールが更新される。このため、上記サイトマップ208に基づいて、監視対象となる通信の種類および／または時間を各モニタエージェント203に配布されることになる。

【0058】

次に、モジュール間の相互情報参照について説明する。図9は、モジュール間の相互情報参照を説明するための説明図である。なお、ここでは説明の便宜上、それぞれ2台の管理マネージャ、モニタエージェントおよびアクションエージェントを設けた場合を示している。

【0059】

すでに説明したように、モニタエージェント203から管理マネージャ202へデータAが送信されると、この管理マネージャ202からアクションエージェント204に対して対策Bが指示されるわけであるが、モニタエージェント20

3～モニタエージェント203'、アクションエージェント204～アクションエージェント204'、管理マネージャ202～管理マネージャ202'の間でも情報の相互参照がおこなわれる。

【0060】

次に、図2に示したデータベース201の自動更新について説明する。図10は、図2に示したデータベース201の自動更新（PULL型）を説明するための説明図である。同図に示すように、データベース201を更新する管理データベース202では、コレクタ部1001がセレクションデータ1002に基づいて、ネットワーク1003に所在するサイトに対してリクエストを発してデータを収集する。具体的には、タイマ1004がタイムアウトした時点で、コレクタ部1001がセレクションデータ1002を読み込み、このセレクションデータ1002に対応するデータをリクエストする。

【0061】

そして、このコレクタ部1001が各サイトから取得したデータをフォーマッタ1005に出力してフォーマット変換などをおこない、その結果をライタ1006がデータベース201に書き込む。

【0062】

ところで、かかるデータベース201の自動更新は必ずしもPULL型でおこなう必要はなく、図11に示すようにPUSH型でおこなうこともできる。かかるPUSH型でデータベース201を自動更新することとすると、ネットワークに存在するサイトからデータベース201に自動的にデータが送り込むことができ、かつ、管理マネージャ202の構成が簡素化することができる。

【0063】

また、図12に示すように、PUSH型システムの管理マネージャ202内にユーザインターフェース1007を設けると、ユーザの発意のもとに所望のサイトに対してリクエストを発することができる。さらに、図13に示すように、PULL型システムの管理マネージャ202内にユーザインターフェース1007を設けると、ネットワークに存在するサイトから自動的に送り込まれたデータをユーザの発意に基づいてデータベース201内に取り込むことができる。

【0064】

次に、図2に示した管理マネージャ202、モニタエージェント203およびアクションエージェント204による処理手順について説明する。まず、モニタエージェント203が異常を検知してからアクションエージェント204が対策を実施するまでの処理手順について説明する。

【0065】

図14は、モニタエージェント203が異常を検知してからアクションエージェント204が対策を実施するまでの処理手順を示すフローチャートである。同図に示すように、モニタエージェント204は、エンティティのログを分析して（ステップS1401）、異常の有無を確認する。その結果、異常を検知した場合には（ステップS1402肯定）、管理マネージャ202に対して異常を通知する（ステップS1403）。

【0066】

そして、管理マネージャ202は、データベース201などを参照して対策および対策依頼先を決定し（ステップS1404）、対策依頼先であるアクションエージェント204に対して対策を依頼する（ステップS1405）。

【0067】

この対策の依頼を受けたアクションエージェント204は、指示された対策を実施し（ステップS1406）、対策結果を管理マネージャ202に対して通知する（ステップS1407）。この対策結果を受け取った管理マネージャ202は、対策結果をディスプレイに表示するなどしてユーザに報告する（ステップS1408）。

【0068】

ところで、ユーザは、エンティティを対策実施前の状態に戻すことを望む場合が多いので、本実施の形態では、かかるエンティティの対策復元も可能としている。図15は、エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャートである。

【0069】

同図に示すように、ユーザが管理マネージャ202のメニューから「対策復元

」を選択し（ステップS1501）、対策を復元するエンティティを指定すると（ステップS1502）、管理マネージャ202は、指定されたエンティティの対策履歴を表示する（ステップS1503）。

【0070】

ここで、ユーザが対策履歴から復元する対策を選択すると（ステップS1504）、管理マネージャ202は、対策依頼先となるアクションエージェント204に対策を依頼する（ステップS1505）。

【0071】

そして、このアクションエージェント204は、依頼された対策を実施して（ステップS1506）、対策結果を管理マネージャ202に通知し（ステップS1507）、管理マネージャ202は、この対策結果をユーザに報告する（ステップS1508）。

【0072】

次に、図2に示した管理マネージャ202における対策ルールの更新手順について説明する。図16は、図2に示した管理マネージャ202における対策ルールの更新手順を説明するための説明図である。同図に示すように、ユーザは、入手した対策ルールを適当な（所定の）ディレクトリに置き（ステップS1601）、管理マネージャ202のメニューから「対策ルール更新」を選択する（ステップS1602）。

【0073】

そして、ユーザが、新しい対策ルールのファイルパス名を指定したならば（ステップS1603）、管理マネージャ202は、オブジェクトの属性、対策ルールファイル名を更新する（ステップS1604）。

【0074】

次に、図2に示した管理マネージャ202において対策プランをカスタマイズする際の処理手順について説明する。図17は、図2に示した管理マネージャ202において対策プランをカスタマイズする際の処理手順を示すフローチャートである。

【0075】

同図に示すように、ユーザが、管理マネージャ202のメニューから「対策プランカスタマイズ」を選択すると（ステップS1701）、管理マネージャ202は、対策プランを編集する対策プランエディタを起動する（ステップS1702）。

【0076】

そして、この対策プランエディタが起動したならば、ユーザは、このエディタを用いて対策プランをカスタマイズし（ステップS1703）、管理マネージャ202は、オブジェクトの属性、対策プランファイル名を更新する（ステップS1704）。

【0077】

次に、分析ルールを更新する際の管理マネージャ202とモニタエージェント203の処理手順について説明する。図18は、分析ルールを更新する際の管理マネージャ202とモニタエージェント203の処理手順を示すフローチャートである。

【0078】

同図に示すように、ユーザが入手した分析ルールを適当なディレクトリに置き（ステップS1801）、管理マネージャ202のメニューから「分析ルール更新」を選択し（ステップS1802）、新しい分析ルールのファイルパス名と、分析ルールを送るモニタエージェント203を指定すると（ステップS1803）、管理マネージャ202は、この分析ルールをモニタエージェント203に配布する（ステップS1804）。

【0079】

その後、このモニタエージェント203は、分析ルール更新し（ステップS1805）、管理マネージャ202に対して更新結果を返し（ステップS1806）、管理マネージャ202は更新結果をユーザに報告する（ステップS1807）。

【0080】

次に、分析ルールをカスタマイズする際の管理マネージャ202とモニタエージェント203の処理手順について説明する。図19は、分析ルールをカスタマ

イズする際の管理マネージャ202とモニタエージェント203の処理手順を示すフローチャートである。

【0081】

同図に示すように、ユーザが管理マネージャ202のメニューから「分析ルールカスタマイズ」を選択し（ステップS1901）、分析ルールをカスタマイズするモニタエージェント203を指定すると（ステップS1902）、管理マネージャ202は、指定されたモニタエージェント203に対して、分析ルールのカスタマイズ可能な部分である分析項目リストを要求する（ステップS1903）。

【0082】

そして、この要求を受けたモニタエージェント203は、管理マネージャ202に対して分析項目リストを送り（ステップS1904）、管理マネージャ202は、分析項目リストを編集する分析項目エディタを起動する（ステップS1905）。

【0083】

その後、ユーザは、この分析項目エディタを用いて分析項目リストをカスタマイズし（ステップS1906）、管理マネージャ202は、カスタマイズした分析項目リストをモニタエージェント203に配布する（ステップS1907）。

【0084】

そして、モニタエージェント203は、分析項目リストを更新した後（ステップS1908）、更新結果を管理マネージャ202に返し（ステップS1909）、管理マネージャ202はカスタマイズ結果をユーザに報告する（ステップS1910）。

【0085】

次に、対策モジュールの更新手順について説明する。図20は、対策モジュールの更新手順を示すフローチャートである。同図に示すように、ユーザが、入手した対策モジュールを適当なディレクトリに置き（ステップS2001）、管理マネージャ202のメニューから「対策モジュール更新」を選択し（ステップS2002）、新しい対策モジュールのファイルパス名と、対策モジュールを送る

アクションエージェント204を指定すると（ステップS2003）、管理マネージャ202は、該当するアクションエージェント204に対して対策モジュールを配布する（ステップS2004）。

【0086】

そして、アクションエージェント204は、対策モジュールを更新したならば（ステップS2005）、更新結果を管理マネージャ202に返し（ステップS2006）、管理マネージャ202が更新結果をユーザに報告する（ステップS2007）。

【0087】

次に、管理マネージャ202とモニタエージェント203との間で授受される検知通知およびACKのデータ構造について説明する。図21は、管理マネージャ202とモニタエージェント203との間で授受される検知通知およびACKのデータ構造の一例を示す図である。

【0088】

同図（a）に示すように、モニタエージェント203は、エンティティの異常を検知した場合に、管理マネージャ202に対して検知通知を送信し、また、モニタエージェント203は、この検知通知を受け付けたならば、モニタエージェント203に対してACKを返す。

【0089】

同図（b）に示すように、この検知通知2101は、OPコード、エージェントID、シーケンス番号、事象識別子、被害識別子、エンティティID、エンティティログ、時刻および対策パラメータからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、シーケンス番号は、モニタエージェント203が検知通知につける通し番号である。また、事象識別子は、モニタエージェント203が検知した事象を一意に識別する情報であり、被害識別子は、モニタエージェント203が検知した事象によって被害を受けたあるいは受ける可能性があるかどうかを示す情報である。また、エンティティIDは、モニタエージェント203が異常を検知したエンティティのIDであり、エンティティログは、モニタエージェント203が検知したエンティティの

ログである。

【0090】

同図(c)に示すように、ACK2102は、OPコードとシーケンス番号からなる。なお、このシーケンス番号は、モニタエージェント203が検知通知につける通し番号である。

【0091】

次に、管理マネージャ202とアクションエージェント204との間で授受される対策依頼および結果通知のデータ構造について説明する。図22は、管理マネージャ202とアクションエージェント204との間で授受される対策依頼および結果通知のデータ構造の一例を示す図である。

【0092】

同図(a)に示すように、モニタエージェント203は、対策および対策依頼先を決定すると、アクションエージェント204に対して対策依頼を送る。一方、アクションエージェント204は、この対策依頼を受け取ると、対策依頼で指定された対策を実施し、管理マネージャ202に対策結果を返す。

【0093】

同図(b)に示すように、この対策依頼2201は、OPコード、エージェントID、シーケンス番号、エンティティID、対策識別子および対策パラメータからなる。ここで、このシーケンス番号は、管理マネージャ202が対策依頼につける通し番号であり、対策識別子は、アクションエージェント204が保有する対策機能を一意に識別する情報であり、対策パラメータは、モニタエージェント203が異常を起こしたエンティティのログをフィールドごとに分割したものである。

【0094】

同図(c)に示すように、結果通知2202は、OPコード、シーケンス番号、エンティティID、戻り値およびエラーコードからなる。ここで、このシーケンス番号は、管理マネージャ202が対策依頼につける通し番号であり、エンティティIDは、アクションエージェント204が設定を変更したエンティティのIDであり、戻り値は、設定変更によりエンティティが返す値である。また、エ

ラーコードは、対策が実施された場合には「E_OK」となり、知らない対策識別子が渡された場合には「E_UNKNOWN」となり、対策パラメータが不足した場合には「E_LESS_ARG」となり、予期しないエラーが発生した場合には「E_UNDEF」となる。

【0095】

次に、管理マネージャ202とモニタエージェント203との間で授受されるDB（分析ルール）配布および結果通知のデータ構造について説明する。図23は、管理マネージャ202とモニタエージェント203との間で授受されるDB（分析ルール）配布および結果通知のデータ構造の一例を示す図である。

【0096】

同図（a）に示すように、モニタエージェント203の分析ルールを更新するために、管理マネージャ202は、モニタエージェント203に対してDB（分析ルール）を配布する。モニタエージェント203は、このDB配布を受け取ると、配布された分析ルールを取り込み、取り込み結果を管理マネージャ202に返す。

【0097】

同図（b）に示すように、このDB配布2301は、OPコード、エージェントIDおよび分析ルールからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、分析ルールは、配布対象となる分析ルールである。

【0098】

同図（c）に示すように、結果通知2302は、OPコード、エージェントIDおよびエラーコードからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布されたルールのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布されたルールが古い場合（同じ判を含む）には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【0099】

次に、管理マネージャ202とモニタエージェント203との間で授受されるリスト要求およびリストのデータ構造について説明する。図24は、管理マネージャ202とモニタエージェント203との間で授受されるリスト要求およびリストのデータ構造の一例を示す図である。

【0100】

同図(a)に示すように、モニタエージェント203の分析項目をカスタマイズするために、管理マネージャ202は、モニタエージェント203に分析項目リストを要求する。このモニタエージェント203は、このリスト要求を受け付けると、分析項目リストを管理マネージャ202に返す。

【0101】

同図(b)に示すように、このリスト要求2401は、OPコードとエージェントIDからなり、このエージェントIDは、エージェントを一意に特定するオブジェクトIDである。

【0102】

同図(c)に示すように、リスト2402は、OPコード、エージェントID、分析項目リストおよびエラーコードからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、分析項目リストは、モニタエージェントの現在の分析項目リストであり、エラーコードは、通常は「E_OK」となり、更新中に予期しないエラーが発生した「E_UNDEF」となる。

【0103】

次に、管理マネージャ202とモニタエージェント203との間で授受されるリスト配布および結果通知のデータ構造について説明する。図25は、管理マネージャ202とモニタエージェント203との間で授受されるリスト配布および結果通知のデータ構造の一例を示す図である。

【0104】

同図(a)に示すように、モニタエージェント203の分析項目をカスタマイズするために、管理マネージャ202は、モニタエージェント203に対して分析項目リストを配布する。モニタエージェント203は、このリスト配布を受け取ると、配布された分析項目リストを取り込み、取り込み結果を管理マネージャ

2 0 2 に返す。

【 0 1 0 5 】

同図（b）に示すように、このリスト配布 2 5 0 1 は、OPコード、エージェントIDおよび分析項目リストからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、分析項目リストは、配布対象となる分析項目リストである。

【 0 1 0 6 】

同図（c）に示すように、結果通知 2 5 0 2 は、OPコード、エージェントIDおよびエラーコードからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布された分析リストのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布された分析リストが古い場合（同じ判を含む）には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【 0 1 0 7 】

次に、管理マネージャ 2 0 2 とアクションエージェント 2 0 4 との間で授受される対策配布および結果通知のデータ構造について説明する。図 2 6 は、管理マネージャ 2 0 2 とアクションエージェント 2 0 4 との間で授受される対策配布および結果通知のデータ構造の一例を示す図である。

【 0 1 0 8 】

同図（a）に示すように、アクションエージェント 2 0 4 の対策モジュールを更新するために、管理マネージャ 2 0 2 は、アクションエージェント 2 0 4 に対して対策モジュールを配布する。アクションエージェント 2 0 4 は、この対策モジュールの配布を受け付けると、配布された対策モジュールを取り込み、取り込み結果を管理マネージャ 2 0 2 に返す。

【 0 1 0 9 】

同図（b）に示すように、この対策配布 2 6 0 1 は、OPコード、エージェントIDおよび対策モジュールからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、対策モジュールは、配布対

象となる対策である。

【0110】

同図(c)に示すように、結果通知2602は、OPコード、エージェントIDおよびエラーコードからなる。ここで、このエージェントIDは、エージェントを一意に特定するオブジェクトIDであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布された対策モジュールのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布された対策モジュールが古い場合(同じ判を含む)には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【0111】

次に、図2に示した管理マネージャ202がおこなう対策決定処理について説明する。図27は、図2に示した管理マネージャ202がおこなう対策決定処理を説明するための説明図である。

【0112】

同図に示す管理マネージャ202は、対策プランを用いた対策および対策依頼先の決定をおこなう。ここで、この対策プランとは、同じ事象識別子を持つ対策ルールが複数ある場合に、どの対策ルールを選択するかを決定するためのルールであり、被害識別子、脅威識別子および対策識別子のタプルで構成される。

【0113】

具体的には、この管理マネージャ202がモニタエージェント203から事象識別子を受け取ると(ステップS2701)、この事象識別子から対策ルールを検索し(ステップS2702)、脅威識別子を取得する(ステップS2703)。そして、別途モニタエージェント203から被害識別子を取得し(ステップS2704)、この被害識別子と脅威識別子から対策プランを検索する(ステップS2705)。

【0114】

そして、検索した対策識別子から対策ルールを検索し(ステップS2706)、対策識別子に基づいてアクションエージェント204を選択し(ステップS2707)、選択したアクションエージェント204に対して対策を指示する。

【0115】

ここで、この被害識別子とは、モニタエージェント203が検知した事象によって、被害を受ける可能性があるかどうかを示す識別子であり、この被害識別子には、「被害あり」、「被害なし」、「判別不能」の3つがある。この被害識別子は、モニタエージェント203が異常を検知したときに、管理マネージャ202に送る検知通知に含まれる。

【0116】

また、脅威識別子とは、モニタエージェント203が検知した事象によって受ける可能性がある被害の種類（大きさ）を示す識別子である。この被害の種類は、事象によって決まり、対策ルールに含まれる。

【0117】

また、対策識別子は、アクションエージェント204で実施できる対策を一意に示す識別子であり、管理マネージャ202がアクションエージェント204に送る対策依頼に含まれる。なお、対策指示子は、管理マネージャ202がどのアクションエージェント204に対策依頼を送るかを示す指示子である。

【0118】

また、事象識別子は、モニタエージェント203が検知した事象を一意に示す識別子である。モニタエージェント203が、異常を検知したときに管理マネージャ202に送る検知通知に含まれる。

【0119】

次に、対策プランの一例について説明する。図28は、対策プランの一例を示す図である。同図に示す対策プランと対策ルールがある場合には、管理マネージャ202は、この対策プランと対策ルールを使って、対策および対策依頼先を決定する。

【0120】

たとえば、同図（a）に示すように、モニタエージェント203が「事象0001」を検知し、「被害あり」と管理マネージャ202に通知した場合には、この管理マネージャ202は、「事象0001」を検索キーとして同図（b）に示す対策ルールを検索する。ここでは、同図（b）に示したように2つの対策ル

ルがヒットすることになるが、脅威識別子は必ず同じものとなる（ここでは「脅威 0 0 0 1」となる）。

【 0 1 2 1 】

そして、管理マネージャ 2 0 2 は、「被害あり」、「脅威 0 0 0 1」を検索キーとして同図（c）に示す対策プランを検索し、対策プランの対策識別子の欄から「対策 0 0 0 1」を選出する。

【 0 1 2 2 】

その後、同図（d）に示すように、2つのヒットした対策ルールのうち、「対策 0 0 0 1」を含むルールを選択し、対策指示子の欄から「SERVER」を対策依頼先として選出する。なお、モニタエージェント 2 0 3 が「事象 0 0 0 1」を検知し、「被害不明」と管理マネージャ 2 0 2 に通知した場合には、対策として「対策 0 0 0 2」が選出されることになる。

【 0 1 2 3 】

このように、この対策ルールは、ある事象に対してとり得る可能性がある対策のすべてを列挙したものであり、対策プランとは、列挙された対策ルールを選択するためのルールであり、被害の有無、被害の大きさによって選択する。なお、かかる対策ルールと対策プランを一つにすることもできるが、被害の有無、被害の大きさによって選択する対策をシステムを運用するサイトのポリシーによってカスタマイズできるようにするために、両者を分けている。このため、ユーザは、対策プランをカスタマイズすることができる。

【 0 1 2 4 】

次に、図 2 に示した管理マネージャ 2 0 2 の機能的な構成について説明する。図 2 9 および図 3 0 は、図 2 に示した管理マネージャ 2 0 2 の機能的な構成を示すブロック図である。

【 0 1 2 5 】

図 2 9 に示すように、管理マネージャ 2 0 2 は、オブジェクト管理部 2 9 0 1、状態監視部 2 9 0 2、プラン構築部 2 9 0 3 およびエージェント機能管理部 2 9 0 4 を有する。

【 0 1 2 6 】

オブジェクト管理部 2901 は、管理マネージャ 202、エージェント、エンティティをそれぞれオブジェクトとして管理する機能部であり、対策ルールおよび対策プランは、管理マネージャオブジェクトの属性として管理する。なお、後述する対策決定部は、対策を決定するために、このオブジェクト管理部 2901 が管理する対策ルールおよび対策プランを検索する。

【0127】

このオブジェクト管理部 2901 は、オブジェクトの構成を管理しており、後述する対策決定部は、対策依頼先を決定するために、このオブジェクト管理部 2901 が管理する構成情報を参照する。

【0128】

状態監視部 2902 は、エージェントの動作状態を確認する機能部である。エージェントに定期的に通信をおこない、通信したときに応答があるか否かでオブジェクト管理部 2901 が管理するエージェントオブジェクトのステータス属性を変更する。

【0129】

プラン構築部 2903 は、対策プランをカスタマイズする機能部であり、このプラン構築部 2903 では、カスタマイズした対策プランの管理をオブジェクト管理部 2901 に依頼する。

【0130】

エージェント機能管理部 2904 は、モニタエージェント 203 の分析ルールを更新またはカスタマイズする機能部であり、アクションエージェント 204 の対策モジュールについても更新する。

【0131】

図 30 に示すように、この管理マネージャ 202 は、オブジェクト管理部 2901、検知通知管理部 2905、対策決定部 2906、対策選択部 2907 および対策依頼部 2908 を有する。

【0132】

検知通知管理部 2905 は、モニタエージェント 203 から送られてくる検知通知を受信および管理する機能部であり、受信した検知通知を対策決定部 290

6に出力する。

【0133】

対策決定部2906は、検知通知管理2905から渡された検知通知から、アクションエージェント204へ依頼する対策および対策依頼先を決定する機能部である。この対策決定部2906は、オブジェクト管理部2901が管理する対策ルールと対策プランを検索して、対策および対策依頼先を決定して、対策依頼部2908に出力する。この対策決定部2906は、対策および対策依頼先を複数選び出し、対策選択部2907に対策のユーザ選択を依頼する。

【0134】

対策選択部2907は、対策決定部2906から渡された複数の対策をユーザに報告し、ユーザに選択を依頼する機能部である。また、ユーザから対策復元要求を受け付け、対策を元に戻す。

【0135】

対策依頼部2908は、対策決定部2906から渡された対策依頼先が示すアクションエージェント204に対して対策決定部2906から受け付けた対策を依頼する機能部である。この対策依頼部2908は、アクションエージェント204の結果通知を受けて、ユーザに対策結果を通知する。また、対策によるエンティティの状態変化を示す対策依頼若しくは対策結果の管理をオブジェクト管理部2901に依頼する。

【0136】

次に、上記オブジェクト管理部2901が管理するオブジェクトの一例について説明する。図31は、管理マネージャオブジェクトを示す図であり、図32は、エージェントオブジェクトを示す図であり、図33は、エンティティオブジェクトを示す図である。

【0137】

図31に示すように、管理マネージャオブジェクトには、管理マネージャ202、対策ルール、対策プラン、ログフォーマット定義、エージェント認定リスト、状態監視、モニタエージェント203およびアクションエージェント204に係るものがある。

【0138】

また、図32に示すように、エージェントオブジェクトには、エージェント、エンティティおよび管理マネージャ202に係るものがあり、図33に示すように、エンティティオブジェクトには、エンティティ、FWエンティティ、モニタエージェント203、アクションエージェント204、対策履歴およびエンティティ固有情報に係るものがある。

【0139】

なお、このオブジェクト管理部2901は、オブジェクトの属性値を定義するオブジェクト定義機能、オブジェクトを削除するオブジェクト削除機能、オブジェクトの属性値を参照するオブジェクト参照機能、オブジェクトの属性値を変更するオブジェクト変更機能、並びに、ユーザが作成されたファイルを置くだけでエージェントの設定を済ませることができるエージェント設定ファイル作成補助機能などを有する。

【0140】

次に、図30に示した対策決定部2906の動作についてさらに詳細に説明する。図34は、図30に示した対策決定部2906による対策決定までの処理手順を示すフローチャートである。

【0141】

同図に示すように、管理マネージャ202は、対策ルールを参照して「脅威識別子」を取得するとともに（ステップS3401）、対策プランを参照して「対策識別子」を取得する（ステップS3402）。

【0142】

そして、対策識別子がOR結合の場合には、ユーザに対策の選択を依頼し（ステップS3403）、ユーザが対策を選択する（ステップS3404）。その後、管理マネージャ202は、対策および対策依頼先を決定し（ステップS3405）、アクションエージェント204の動作状態を確認する（ステップS3406）。

【0143】

次に、図30に示した対策決定部2906の構成について説明する。図35は

、図30に示した対策決定部2906の構成を示す機能ブロック図である。同図に示すように、この対策決定部2906は、検知通知管理部2905、オブジェクト管理部2901、対策依頼部2908および対策選択部2907の間に介在し、対策決定機能制御部3501と、対策ルール検索部3502と、対策プラン検索部3503と、状態確認部3504と、対策決定待ちキュー管理部3505と、対策決定待ちキュー3506とからなる。

【0144】

対策決定機能制御部3501は、対策決定機能を制御する機能部であり、対策ルール検索部3502は、対策ルールを検索する機能部であり、対策プラン検索部3503は、対策プランを検索する機能部であり、状態確認部3504は、状態確認をおこなう機能部であり、対策決定待ちキュー管理部3505は、対策決定待ちキュー3506を管理する機能部である。

【0145】

次に、レポーティング機能について説明する。図36は、レポーティング機能を説明するための説明図である。同図に示すように、監視対象を検知エンジンで検知する際に、実装情報3601、運用管理情報3602およびセキュリティ情報3603に基づいて判定をおこない、検知通知をおこなう。すなわち、監視対象サイトの情報（構成、稼働中サービス、セキュリティ機能など）をもとに、多面的な運用状況を判定して報告している。

【0146】

また、かかる実装情報3601、運用管理情報3602およびセキュリティ情報3603は、図37に示すように、防御策を判定する際にも用いられており、防御策リストから防御策を判定する際に、これらの情報を参照して多面的に防御策を選択し、状況に応じた動的な防御を実施している。ここで実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能である。

【0147】

さらに、図38に示すように、これらの実装情報3601、運用管理情報3602およびセキュリティ情報3603は、プロトコル階層間のフィルタとしても

利用される。すなわち、IP層とTCP層との間、TCP層とHTTP層の間、HTTP層とMIMEデータの間、MIMEデータとCGI-APの間のフィルタとして用いることにより、各階層の不正アクセス手口を限定し、解析・検知コストの軽減を図ることができる。

【0148】

また、正常なリクエスト以外を他層に渡さないようフィルタリングすることにより、攻撃に対する防御を実現することができる。さらに、監視対象に関する情報（システム構成、稼働サービス、セキュリティ機能）を参考にし、判定処理の信頼性や妥当性を向上させることもできる。

【0149】

次に、これらの実装情報3601、運用管理情報3602およびセキュリティ情報3603を用いた統合連携管理について説明する。図39は、実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図である。

【0150】

同図に示すように、セキュリティ情報3603は不正手口へとつながり、運用管理情報はサイト情報へとつながり、実装情報はソフト情報へとつながる。ここで、これらの不正手口、サイト情報およびソフト情報は、検知、被害予想・把握、防御・回避・復旧をおこなううえで重要な役割を果たしている。

【0151】

換言すれば、検知（攻撃検知、予兆検知、攻撃予知）をおこなうためには、不正手口、サイト情報およびソフト情報といった総合的な情報が必要であり、また被害予想・把握をおこなったり、防御・回避・復旧をおこない際にも同様の総合的な情報が必要となる。このため、本実施の形態では、実装情報3601、運用管理情報3602およびセキュリティ情報3603を用いた統合連携制御をおこなっている。

【0152】

上述してきたように、本実施の形態によれば、モニタエージェント203でエンティティのログを分析し、異常の予兆を検知した場合には、管理マネージャ2

02に通知する。そして、この管理マネージャ202は、データベース201などに基づいて対策および対策依頼先を決定し、対策依頼先であるアクションエージェント204に該当する対策を実施させるよう構成したので、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる。

【0153】

(付記1) 通信要求を監視する通信要求監視手段と、前記通信要求監視手段から通知された情報に基づいて対策を選択する管理手段と、前記管理手段からの指示に応答して対策を実施する実施手段とを有し、

前記管理手段は、

前記通信要求監視手段からの通知内容と前記実施手段が実施する対策とを対応づけて管理するデータベースと、

前記データベースに基づいて対策を選択する選択手段と、

を備えたことを特徴とする情報管理システム。

【0154】

(付記2) 攻撃事象若しくは漏洩事象の進行過程における2以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集手段と、前記情報収集手段により収集整理された情報を前記データベースに反映する反映手段と、をさらに備えたことを特徴とする付記1に記載の情報管理システム。

【0155】

(付記3) 前記選択手段は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする付記1または2に記載の情報管理システム。

【0156】

(付記4) 前記実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能であることを特徴とする付記3に記載の情報管理システム。

【0157】

(付記5) 複数の通信要求監視手段、管理手段および実施手段をそれぞれ

備えたことを特徴とする付記 1 ～ 4 のいずれか一つに記載の情報管理システム。

【 0 1 5 8 】

(付記 6) 前記複数の通信要求監視手段、管理手段および実施手段が同機種または異機種間でそれぞれ相互に連携して情報交換をおこなうことを特徴とする付記 5 に記載の情報管理システム。

【 0 1 5 9 】

(付記 7) 前記通信要求監視手段により通知される情報および／または前記管理手段により選択される対策に重み付けをおこなうことを特徴とする付記 1 ～ 6 のいずれか一つに記載の情報管理システム。

【 0 1 6 0 】

(付記 8) 前記重み付けする重み係数は、ユーザによって任意に設定できることを特徴とする付記 7 に記載の情報管理システム。

【 0 1 6 1 】

(付記 9) 前記重み付けする重み係数は、前記実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定されることを特徴とする付記 7 に記載の情報管理システム。

【 0 1 6 2 】

(付記 1 0) 前記データベースは、前記通信要求監視手段により通知される情報を時系列で保持し、前記選択手段は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする付記 1 ～ 9 のいずれか一つに記載の情報管理システム。

【 0 1 6 3 】

(付記 1 1) 前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成手段をさらに備えたことを特徴とする付記 1 ～ 1 0 のいずれか一つに記載の情報管理システム。

【 0 1 6 4 】

(付記 1 2) 前記サイトマップ生成手段により生成されたサイトマップに基づいて、監視対象となる通信の種類および／または時間を前記複数の通信要求

監視手段に通知する監視条件通知手段をさらに備えたことを特徴とする付記 1 ～ 10 のいずれか一つに記載の情報管理システム。

【0165】

(付記 13) 前記管理手段は、ネットワークに所在するサイトに対してリクエストを発し、該リクエストに応答して返信される情報に基づいて前記データベースを自動更新することを特徴とする付記 1 ～ 12 のいずれか一つに記載の情報管理システム。

【0166】

(付記 14) 前記リクエストは、ユーザの要求に応答しておこなうことを特徴とする付記 13 に記載の情報管理システム。

【0167】

(付記 15) 前記管理手段は、ネットワークに所在するサイトから自動的に送信される情報に基づいて前記データベースを自動更新することを特徴とする付記 1 ～ 12 のいずれか一つに記載の情報管理システム。

【0168】

(付記 16) ネットワークに所在するサイトから自動的に送信される情報をユーザの要求に応答して前記データベースに取り込むことを特徴とする付記 15 に記載の情報管理システム。

【0169】

(付記 17) システムの脆弱性を示す脆弱性呈示手段と、前記脆弱性呈示手段に対する攻撃に関する情報を収集する情報収集手段と、をさらに備えたことを特徴とする付記 1 ～ 16 のいずれか一つに記載の情報管理システム。

【0170】

(付記 18) 通信内容の発信元を調査する調査手段と、前記調査手段による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定手段と、をさらに備えたことを特徴とする付記 1 ～ 17 のいずれか一つに記載の情報管理システム。

【0171】

(付記 19) 攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、

前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに備えたことを特徴とする付記 1 ～ 1 8 のいずれか一つに記載の情報管理システム。

【 0 1 7 2 】

(付記 2 0) 通信要求を監視部によって監視する通信要求監視工程と、
前記通信要求監視工程により通知される通知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、
前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、
を含んだことを特徴とする情報管理方法。

【 0 1 7 3 】

(付記 2 1) 攻撃事象若しくは漏洩事象の進行過程における 2 以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集工程と、前記情報収集工程により収集整理された情報を前記データベースに反映する反映工程と、をさらに含んだことを特徴とする付記 2 0 に記載の情報管理方法。

【 0 1 7 4 】

(付記 2 2) 前記選択工程は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする付記 2 0 または 2 1 に記載の情報管理方法。

【 0 1 7 5 】

(付記 2 3) 前記実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能であることを特徴とする付記 2 2 に記載の情報管理方法。

【 0 1 7 6 】

(付記 2 4) 複数の監視部、管理部および実施部をそれぞれ設けたことを特徴とする付記 2 0 ～ 2 3 のいずれか一つに記載の情報管理方法。

【 0 1 7 7 】

(付記 2 5) 前記複数の監視部、管理部および実施部が同機種または異機種間でそれぞれ相互に連携して情報交換をおこなうことを特徴とする付記 2 4 に記載の情報管理方法。

【 0 1 7 8 】

(付記 2 6) 前記監視部により通知される情報および／または前記管理部により選択される対策に重み付けをおこなうことを特徴とする付記 2 0 ～ 2 5 のいずれか一つに記載の情報管理方法。

【 0 1 7 9 】

(付記 2 7) 前記重み付けする重み係数は、ユーザによって任意に設定できることを特徴とする付記 2 6 に記載の情報管理方法。

【 0 1 8 0 】

(付記 2 8) 前記重み付けする重み係数は、前記実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定されることを特徴とする付記 2 6 に記載の情報管理方法。

【 0 1 8 1 】

(付記 2 9) 前記データベースは、前記監視部により通知される情報を時系列で保持し、前記選択工程は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする付記 2 0 ～ 2 8 のいずれか一つに記載の情報管理方法。

【 0 1 8 2 】

(付記 3 0) 前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成工程をさらに含んだことを特徴とする付記 2 0 ～ 2 9 のいずれか一つに記載の情報管理方法。

【 0 1 8 3 】

(付記 3 1) 前記サイトマップ生成工程により生成されたサイトマップに基づいて、監視対象となる通信の種類および／または時間を前記複数の監視部に通知する監視条件通知工程をさらに含んだことを特徴とする付記 2 0 ～ 2 9 のいずれか一つに記載の情報管理方法。

【 0 1 8 4 】

(付記 3 2) 前記管理部が、ネットワークに所在するサイトに対してリクエストを発し、該リクエストに応答して返信される情報に基づいて前記データベースを自動更新することを特徴とする付記 2 0 ～ 3 1 のいずれか一つに記載の情

報管理方法。

【0185】

(付記33) 前記リクエストは、ユーザの要求に応答しておこなうことを特徴とする付記32に記載の情報管理方法。

【0186】

(付記34) 前記管理部が、ネットワークに所在するサイトから自動的に送信される情報に基づいて前記データベースを自動更新することを特徴とする付記20～31のいずれか一つに記載の情報管理方法。

【0187】

(付記35) ネットワークに所在するサイトから自動的に送信される情報をユーザの要求に応答して前記データベースに取り込むことを特徴とする付記34に記載の情報管理方法。

【0188】

(付記36) システムの脆弱性を示す脆弱性呈示工程と、前記脆弱性呈示工程に対する攻撃に関する情報を収集する情報収集工程と、をさらに含んだことを特徴とする付記20～35のいずれか一つに記載の情報管理方法。

【0189】

(付記37) 通信内容の発信元を調査する調査工程と、前記調査工程による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定工程と、をさらに含んだことを特徴とする付記20～36のいずれか一つに記載の情報管理方法。

【0190】

(付記38) 攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに含んだことを特徴とする付記20～37のいずれか一つに記載の情報管理方法。

【0191】

(付記39) 通信要求を監視部によって監視する通信要求監視工程と、前記通信要求監視工程により通知される通知知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、

前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、
をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【 0 1 9 2 】

【発明の効果】

以上説明したように、請求項 1、9 および 10 の発明によれば、データベース内に通知内容と対策を対応づけて保持しておき、通信要求監視手段が通信要求を監視して異常を検知して管理手段に通知すると、この管理手段が、データベースから対策を選択して、実施手段に対策を実行させるよう構成したので、対策を効率良く実行することができ、もって、実際の攻撃に適切な対策を施して被害の極小化を図ることができる。

【 0 1 9 3 】

また、請求項 2 の発明によれば、攻撃事象若しくは漏洩事象の進行過程における 2 以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベースに反映するよう構成したので、データベースの内容を充実させ、より適切な対策を選択することができる。

【 0 1 9 4 】

また、請求項 3 の発明によれば、データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することとしたので、データベースのみならずシステムを取り巻く環境を考慮した上で妥当な対策を未然に実行し、もって被害を極小化することができる。

【 0 1 9 5 】

また、請求項 4 の発明によれば、データベースが通信要求監視手段により通知される情報を時系列で保持し、このデータベースに記憶した時系列の情報に基づいて対策を選択するよう構成したので、時系列的な情報を用いて対策を選択することができる。

【 0 1 9 6 】

また、請求項 5 の発明によれば、複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するよう構成した

ので、空間的な情報を用いて対策を選択することができる。

【 0 1 9 7 】

また、請求項 6 の発明によれば、システムの脆弱性を明示的に呈示し、この脆弱箇所に対する攻撃に関する情報を収集するよう構成したので、悪意者による攻撃手法を把握することができる。

【 0 1 9 8 】

また、請求項 7 の発明によれば、通信内容の発信元を調査した調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定するよう構成したので、踏み台とされているサイトを効率良く特定することができる。

【 0 1 9 9 】

また、請求項 8 の発明によれば、攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、この攻撃対象サイトへの攻撃を回避させるおとりサイトを設けるよう構成したので、攻撃対象サイトの保全を図るとともに攻撃手法を把握することができる。

【図面の簡単な説明】

【図 1】

この発明の実施の形態に係る全体システムに採用した各種技術を説明するための説明図である。

【図 2】

本実施の形態に係る情報管理システムの基本構成を示すブロック図である。

【図 3】

モニタエージェントおよびアクションエージェントを複数設けた場合の構成を示すブロック図である。

【図 4】

管理マネージャが重み付けしたデータ A と重み付けした対策 B を対応づけて保持した場合を示すブロック図である。

【図 5】

図 4 に示したモニタエージェントの構成を示すブロック図である。

【図 6】

図 2 に示した管理マネージャを説明するための説明図である。

【図 7】

図 2 に示した管理マネージャによる物理マップの作成を説明するための説明図である。

【図 8】

図 2 に示した管理マネージャからモニタエージェントに対するフィードバックを説明するための説明図である。

【図 9】

モジュール間の相互情報参照を説明するための説明図である。

【図 1 0】

図 2 に示したデータベースの自動更新（P U L L 型）を説明するための説明図である。

【図 1 1】

図 2 に示したデータベースの自動更新（P U S H 型）を説明するための説明図である。

【図 1 2】

人手を介した場合を含むデータベースの自動更新（P U L L 型）を説明するための説明図である。

【図 1 3】

人手を介した場合を含むデータベースの自動更新（P U S H 型）を説明するための説明図である。

【図 1 4】

モニタエージェントが異常を検知してからアクションエージェントが対策を実施するまでの処理手順を示すフローチャートである。

【図 1 5】

エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャートである。

【図 1 6】

図 2 に示した管理マネージャにおける対策ルールの更新手順を説明するための

説明図である。

【図 1 7】

図 2 に示した管理マネージャにおいて対策プランをカスタマイズする際の処理手順を示すフローチャートである。

【図 1 8】

分析ルールを更新する際の管理マネージャとモニタエージェントの処理手順を示すフローチャートである。

【図 1 9】

分析ルールをカスタマイズする際の管理マネージャとモニタエージェントの処理手順を示すフローチャートである。

【図 2 0】

対策モジュールの更新手順を示すフローチャートである。

【図 2 1】

管理マネージャとモニタエージェントとの間で授受される検知通知および A C K のデータ構造の一例を示す図である。

【図 2 2】

管理マネージャとアクションエージェントとの間で授受される対策依頼および結果通知のデータ構造の一例を示す図である。

【図 2 3】

管理マネージャとモニタエージェントとの間で授受される D B （分析ルール）配布および結果通知のデータ構造の一例を示す図である。

【図 2 4】

管理マネージャとモニタエージェントとの間で授受されるリスト要求およびリストのデータ構造の一例を示す図である。

【図 2 5】

管理マネージャとモニタエージェントとの間で授受されるリスト配布および結果通知のデータ構造の一例を示す図である。

【図 2 6】

管理マネージャとアクションエージェントとの間で授受される対策配布および

結果通知のデータ構造の一例を示す図である。

【図 2 7】

図 2 に示した管理マネージャがおこなう対策決定処理を説明するための説明図である。

【図 2 8】

対策プランの一例を示す図である。

【図 2 9】

図 2 に示した管理マネージャの機能的な構成を示すブロック図である。

【図 3 0】

図 2 に示した管理マネージャの機能的な構成を示すブロック図である。

【図 3 1】

管理マネージャオブジェクトを示す図である。

【図 3 2】

エージェントオブジェクトを示す図である。

【図 3 3】

エンティティオブジェクトを示す図である。

【図 3 4】

図 3 0 に示した対策決定部による対策決定までの処理手順を示すフローチャートである。

【図 3 5】

図 3 0 に示した対策決定部の構成を示す機能ブロック図である。

【図 3 6】

レポート機能の説明するための説明図である。

【図 3 7】

実装情報などを用いた多面的な防御策選択を説明するための説明図である。

【図 3 8】

実装情報などをプロトコル階層間のフィルタとして用いる概念を説明するための説明図である。

【図 3 9】

実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図である。

【符号の説明】

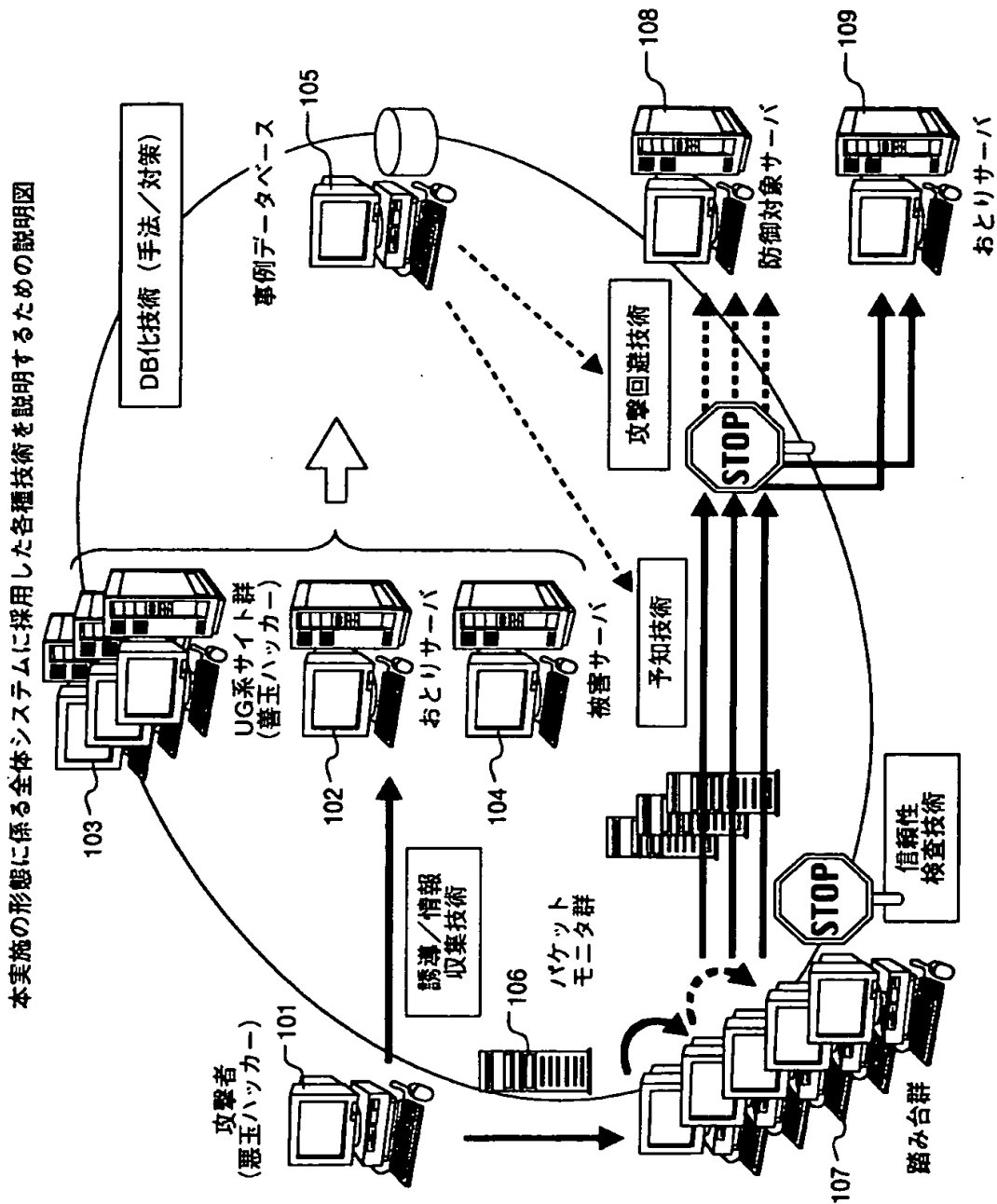
- 101 攻撃者（悪玉ハッカー）
- 102 おとりサーバ
- 103 UG系サイト群（善玉ハッカー）
- 104 被害サーバ
- 105 事例データベース
- 106 パケットモニタ群
- 107 踏み台群
- 108 防御対象サーバ
- 109 おとりサーバ
- 201 データベース
- 202 管理マネージャ
- 203 モニタエージェント
 - 203a データ解析部
 - 203b データ分析部
 - 203c データスタック
 - 203d 重みテーブル
 - 203e 判定処理部
 - 203f 通知部
- 204 アクションエージェント
- 205 システム構成
- 206 運用状況
- 207 モジュール
- 208 サイトの物理マップ
 - 1001 コレクタ部
 - 1002 セレクションデータ
 - 1003 ネットワーク

1 0 0 4 タイマ
1 0 0 5 フォーマッタ
1 0 0 6 ライタ
1 0 0 7 ユーザインターフェース
2 1 0 1 検知通知
2 1 0 2 A C K
2 2 0 1 対策依頼
2 2 0 2 結果通知
2 3 0 1 D B 配布
2 3 0 2 結果通知
2 4 0 1 リスト要求
2 4 0 2 リスト
2 5 0 1 リスト配布
2 5 0 2 結果通知
2 6 0 1 対策配布
2 6 0 2 結果通知
2 9 0 1 オブジェクト管理部
2 9 0 2 状態監視部
2 9 0 3 プラン構築部
2 9 0 4 エージェント機能管理部
2 9 0 5 検知通知管理部
2 9 0 6 対策決定部
2 9 0 7 対策選択部
2 9 0 8 対策依頼部

【書類名】

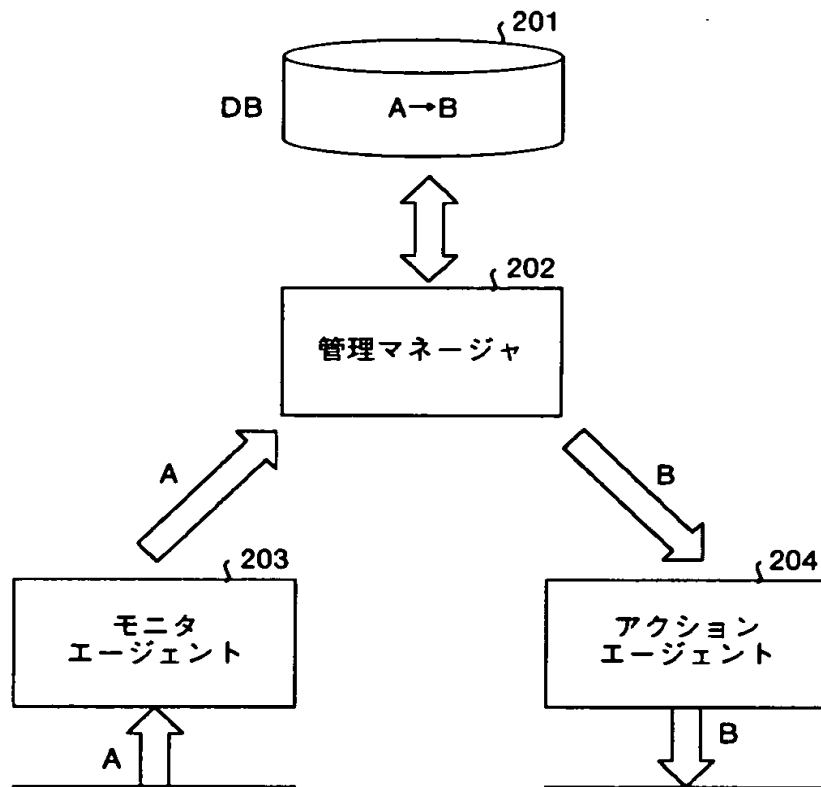
凶面

【図 1】



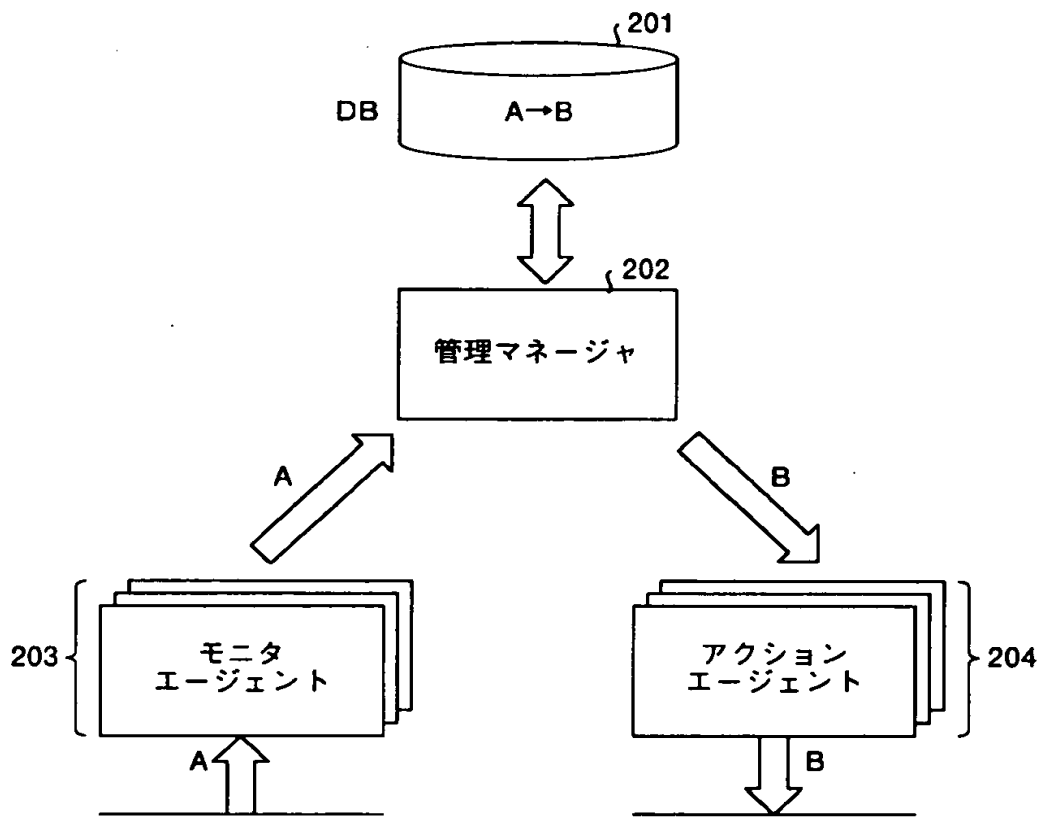
【図 2】

本実施の形態に係る情報管理システムの基本構成を示すブロック図



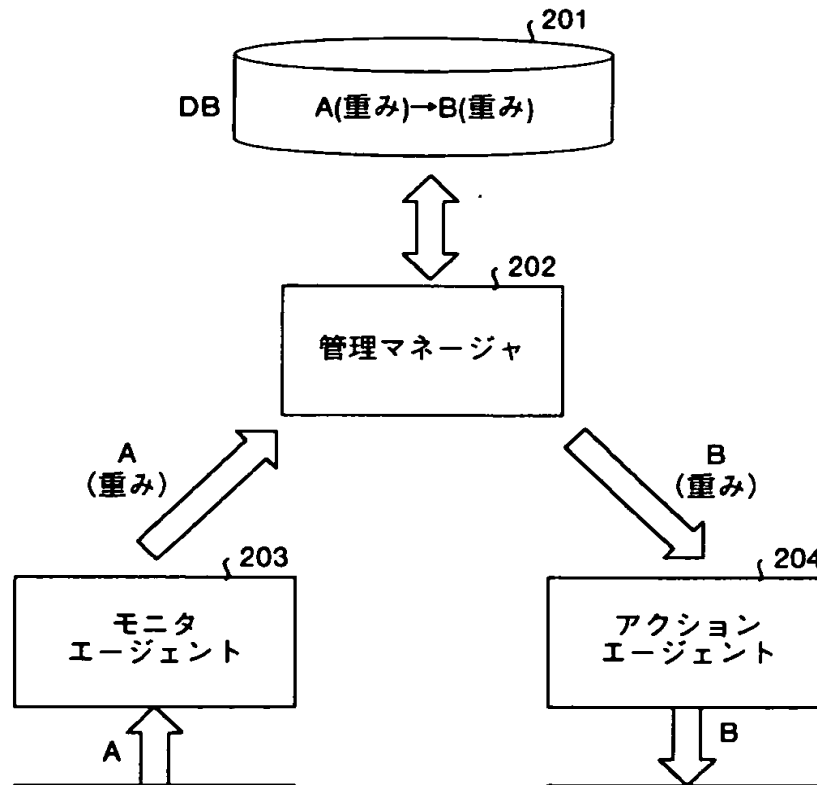
【図 3】

モニタエージェントおよび
アクションエージェントを複数設けた場合の構成を示すブロック図



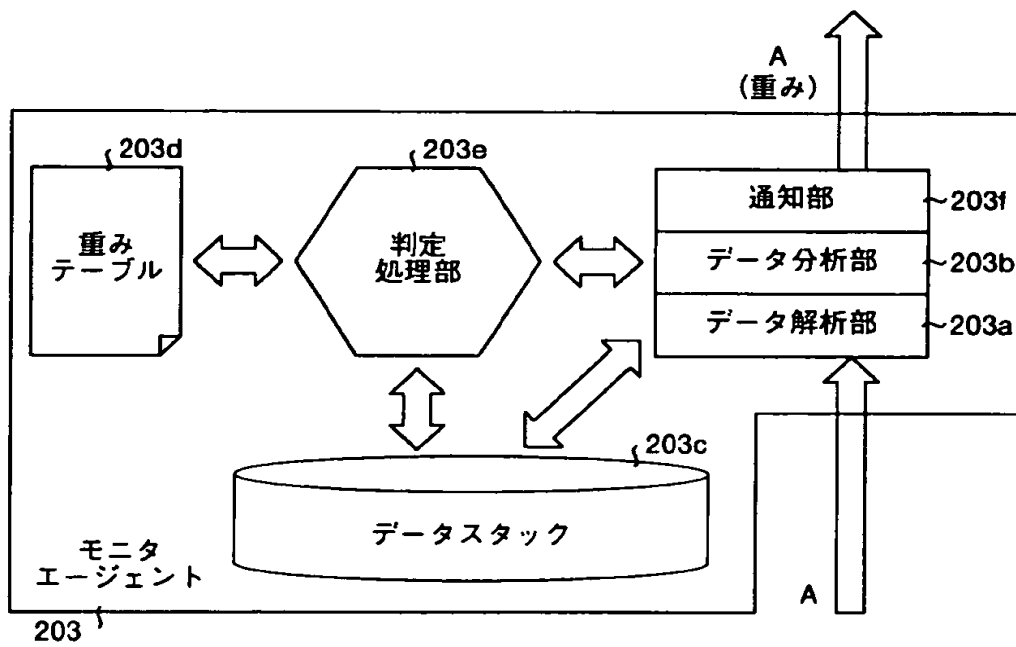
【図4】

管理マネージャが重み付けしたデータAと
重み付けした対策Bを対応づけて保持した場合を示すブロック図



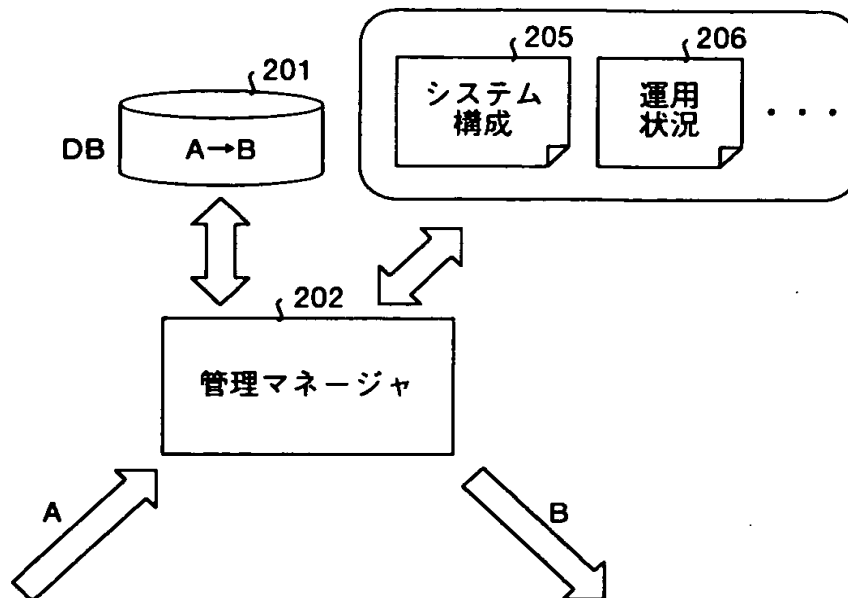
【図 5】

モニタエージェントの構成を示すブロック図



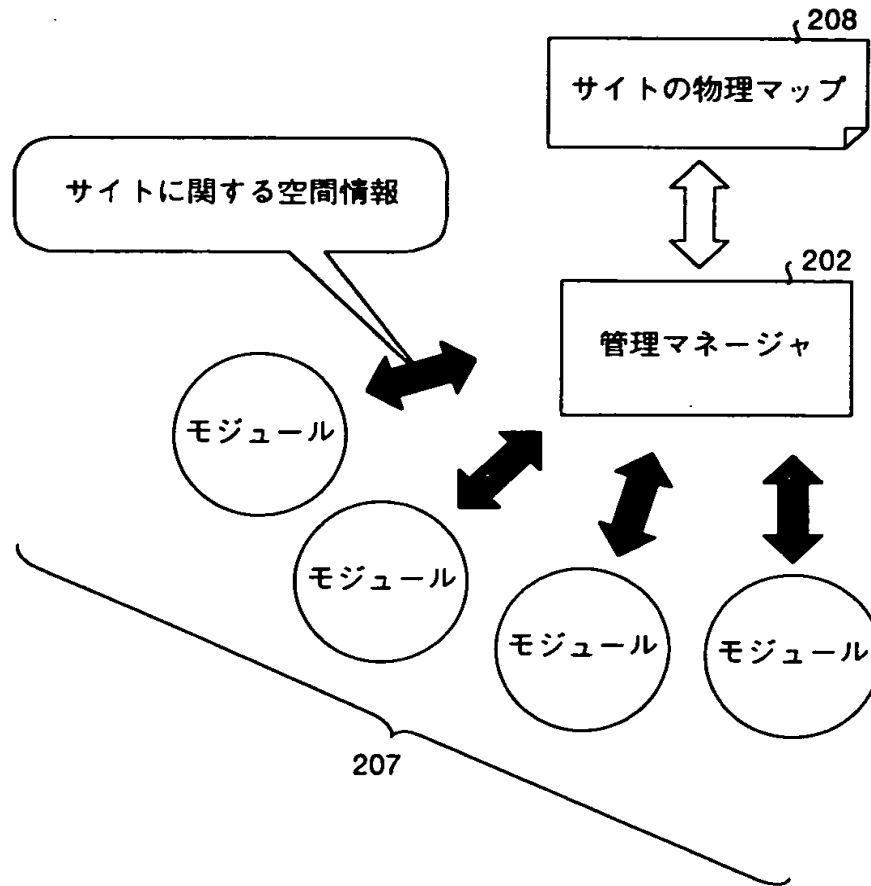
【図 6】

管理マネージャを説明するための説明図



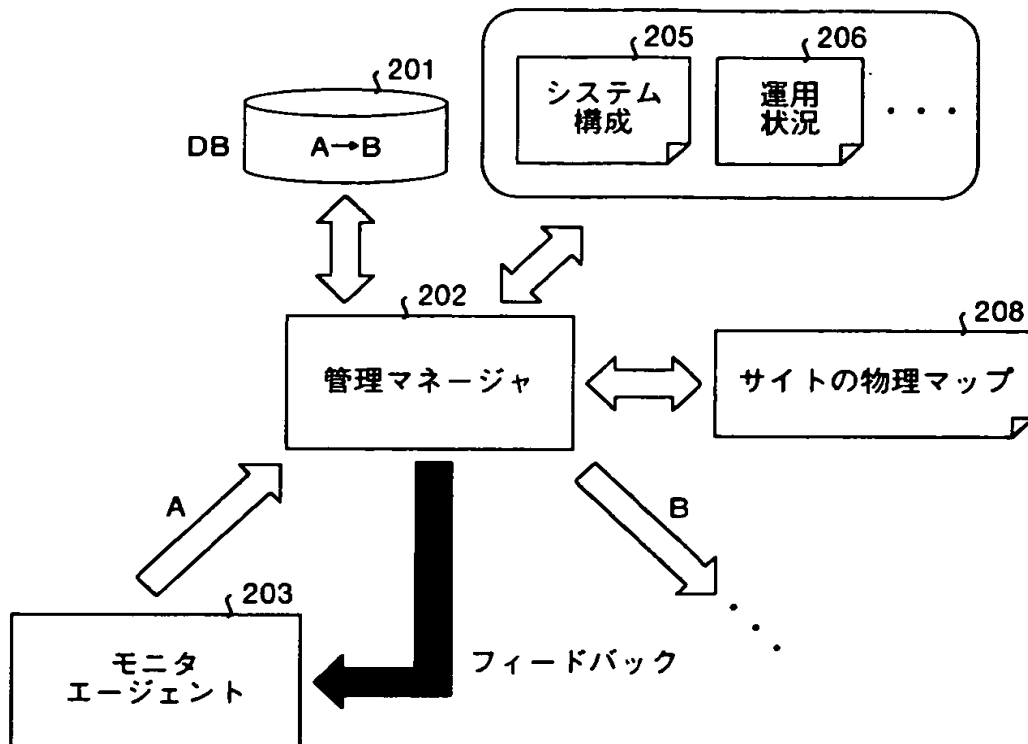
【図 7】

管理マネージャによる物理マップの作成を説明するための説明図



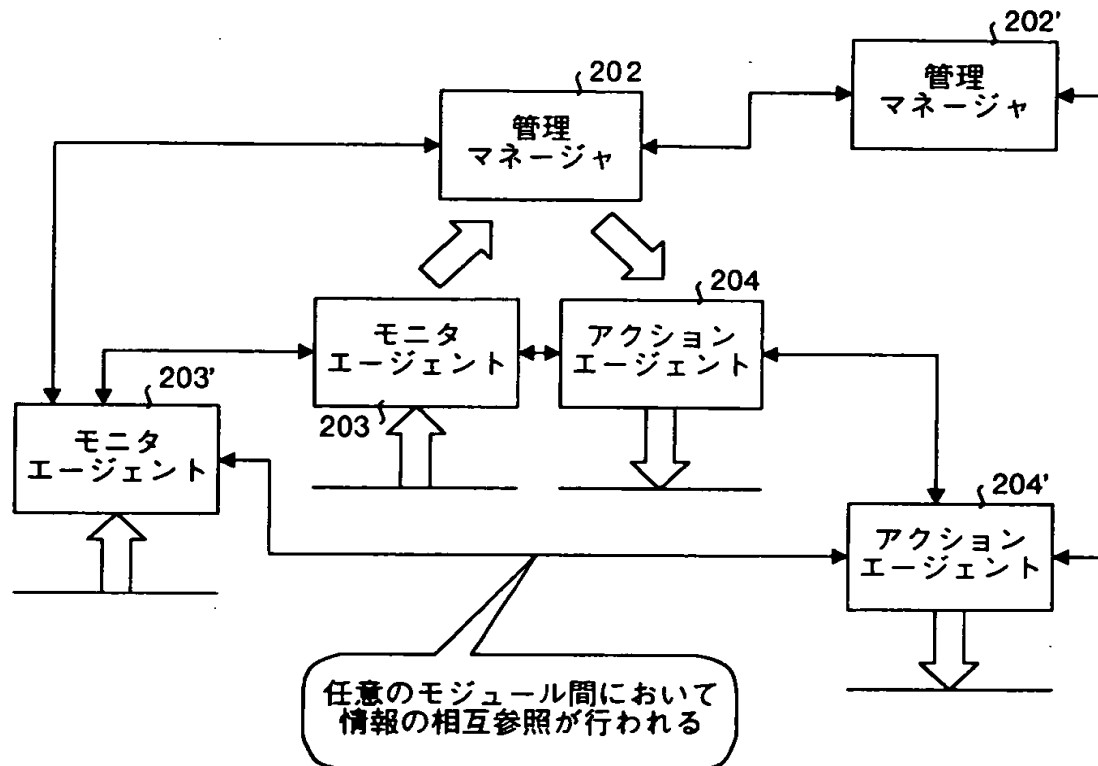
【図 8】

管理マネージャからモニタエージェントに対する
フィードバックを説明するための説明図



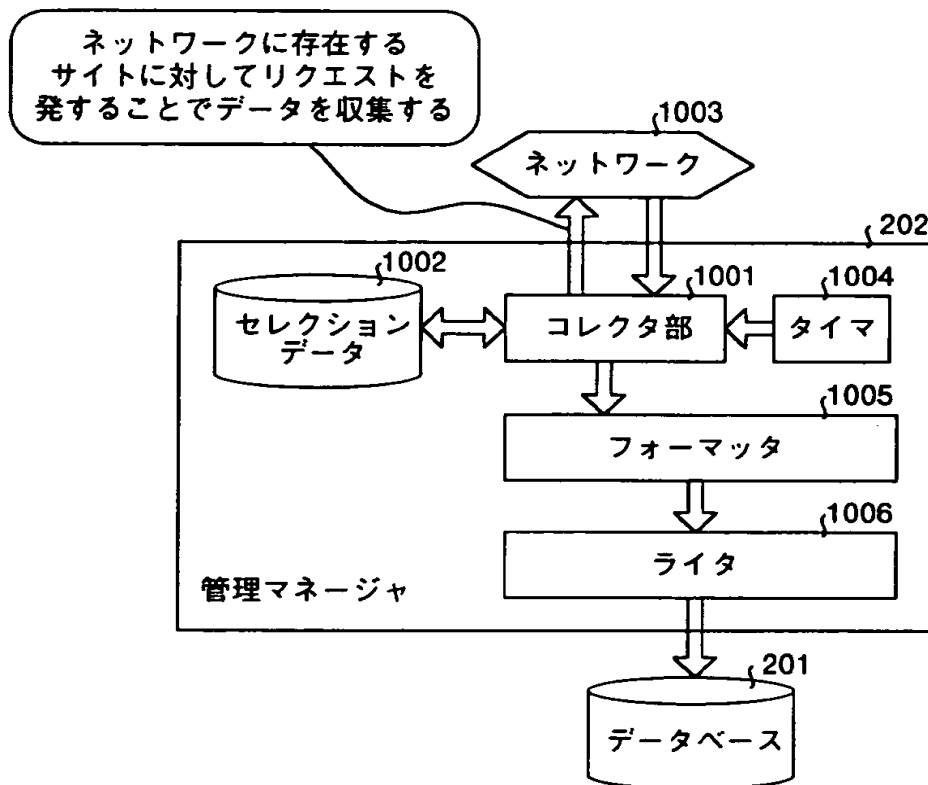
【図 9】

モジュール間の相互情報参照を説明するための説明図



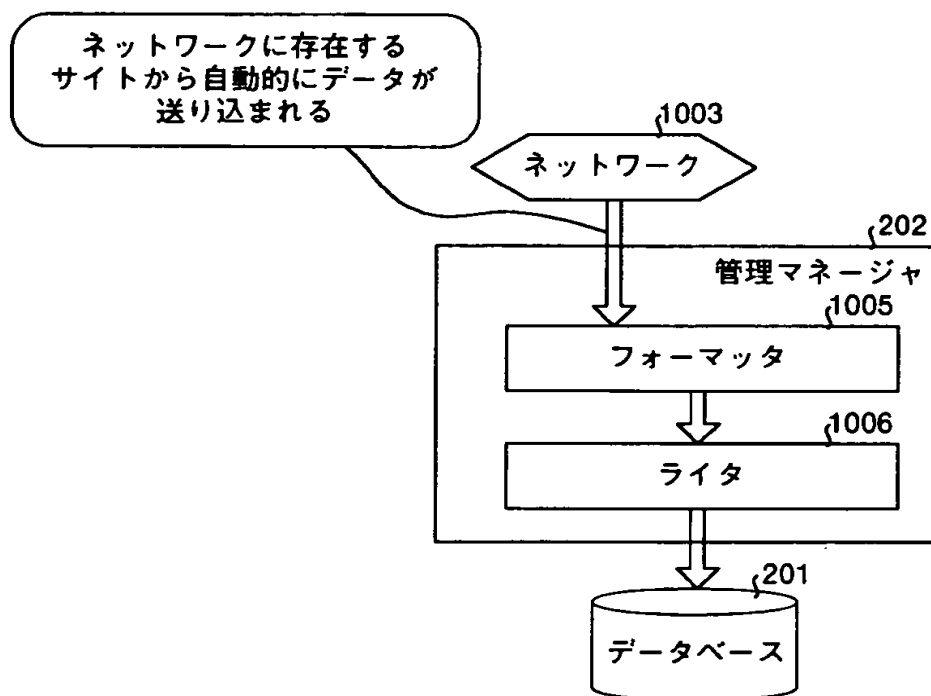
【図10】

データベースの自動更新（PULL型）を説明するための説明図



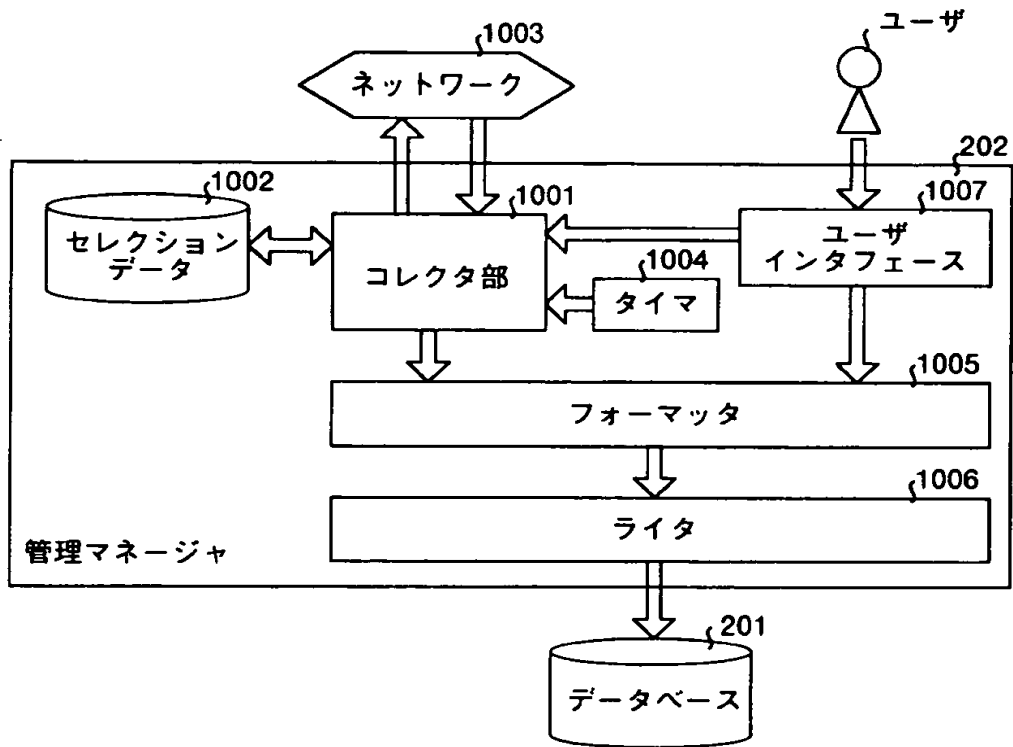
【図 11】

データベースの自動更新（PUSH型）を説明するための説明図



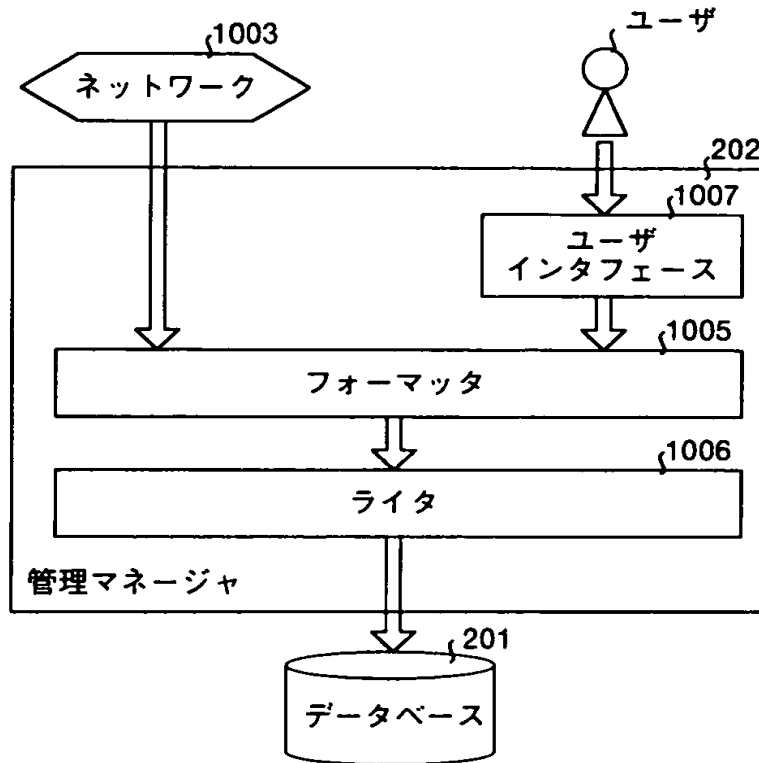
【図 1 2】

人手を介した場合を含むデータベースの自動更新（PULL型）を説明するための説明図



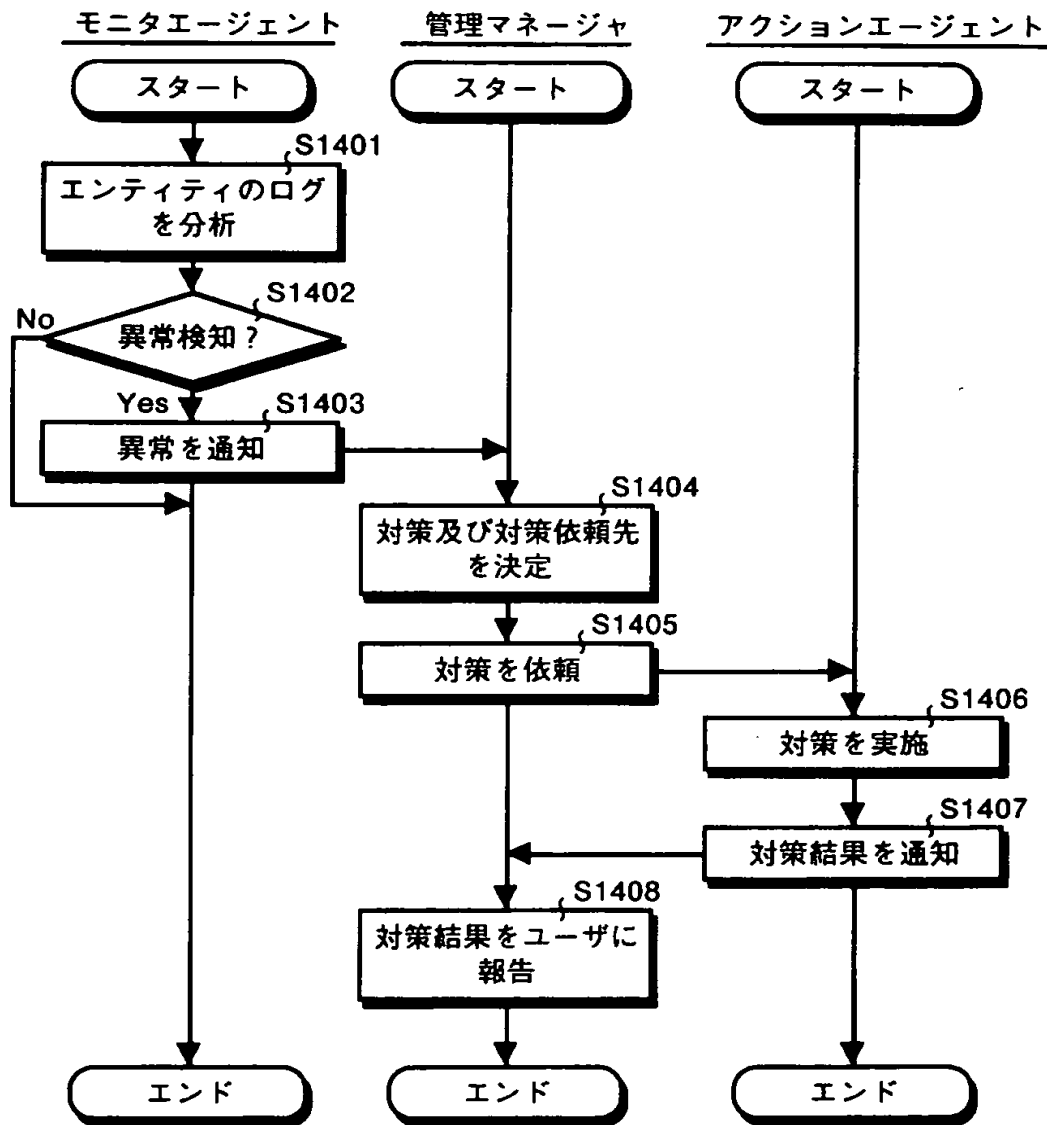
【図13】

人手を介した場合を含むデータベースの自動更新（PUSH型）を説明するための説明図



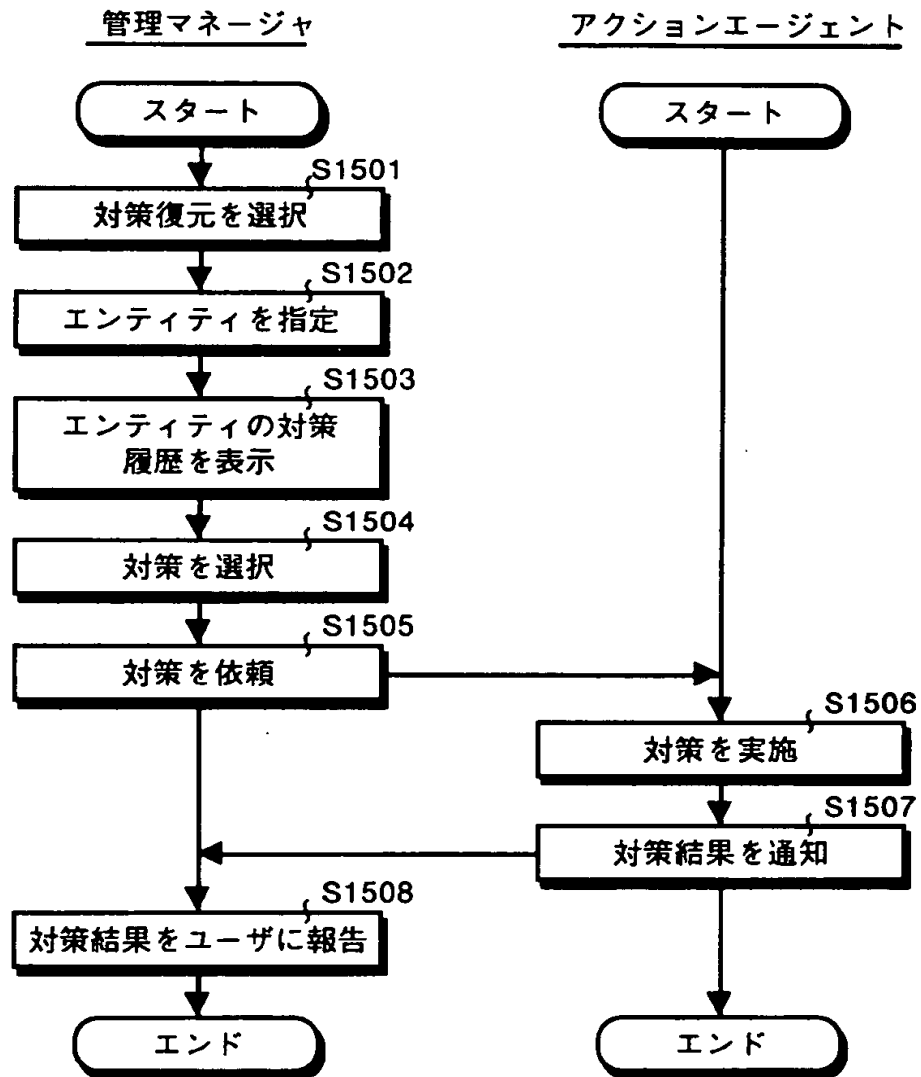
【図 14】

モニタエージェントが異常を検知してからアクションエージェントが
対策を実施するまでの処理手順を示すフローチャート



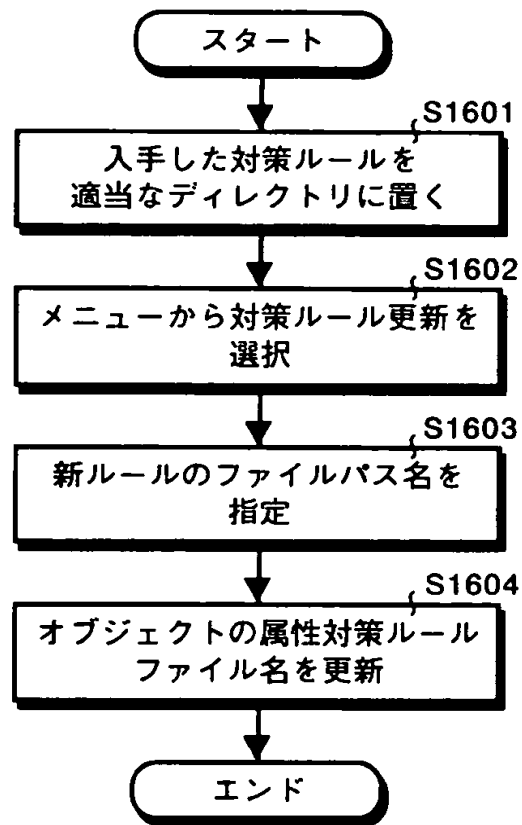
【図15】

エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャート



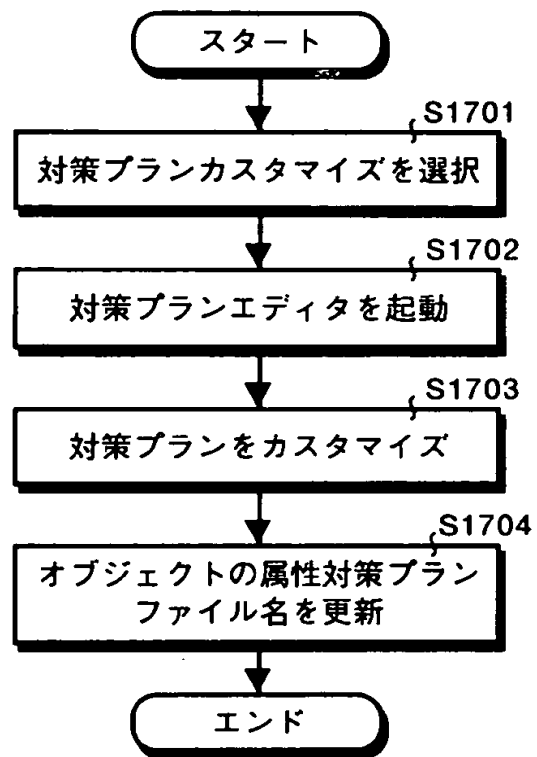
【図 1 6】

管理マネージャにおける対策ルールの更新手順を説明するための説明図



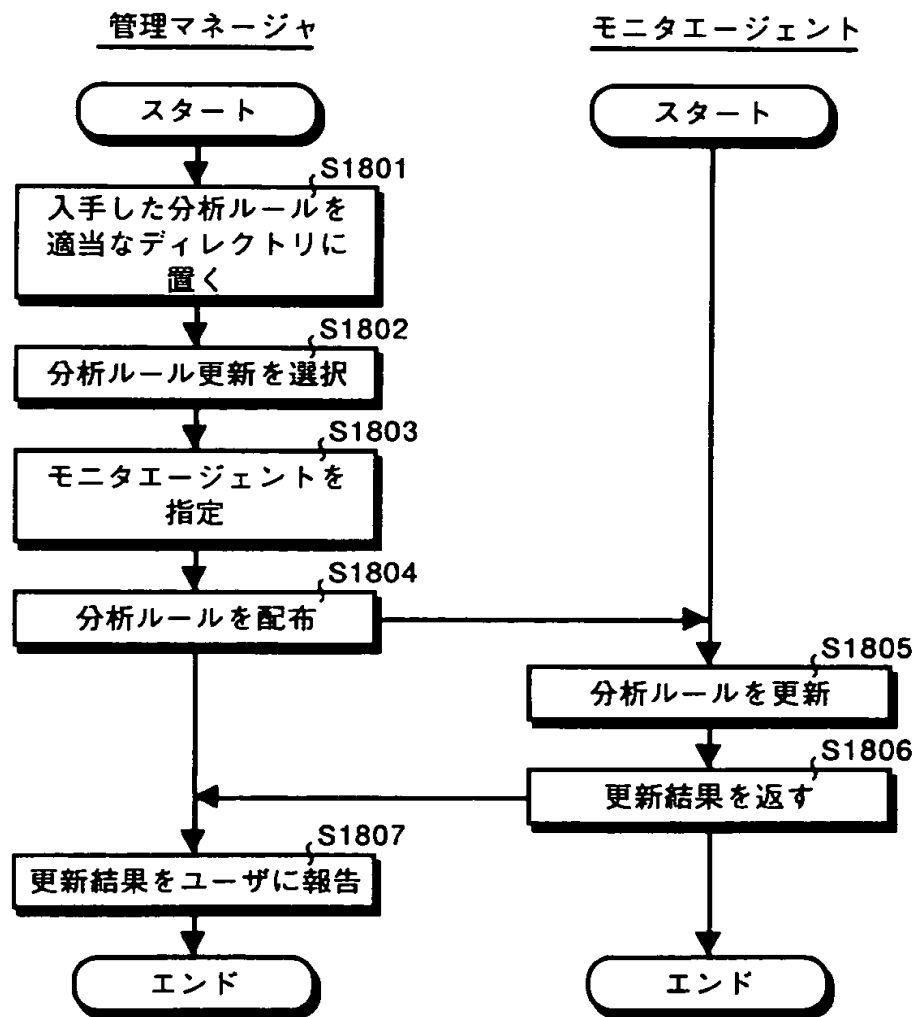
【図 17】

管理マネージャにおいて対策プランをカスタマイズする際の処理手順を示すフローチャート



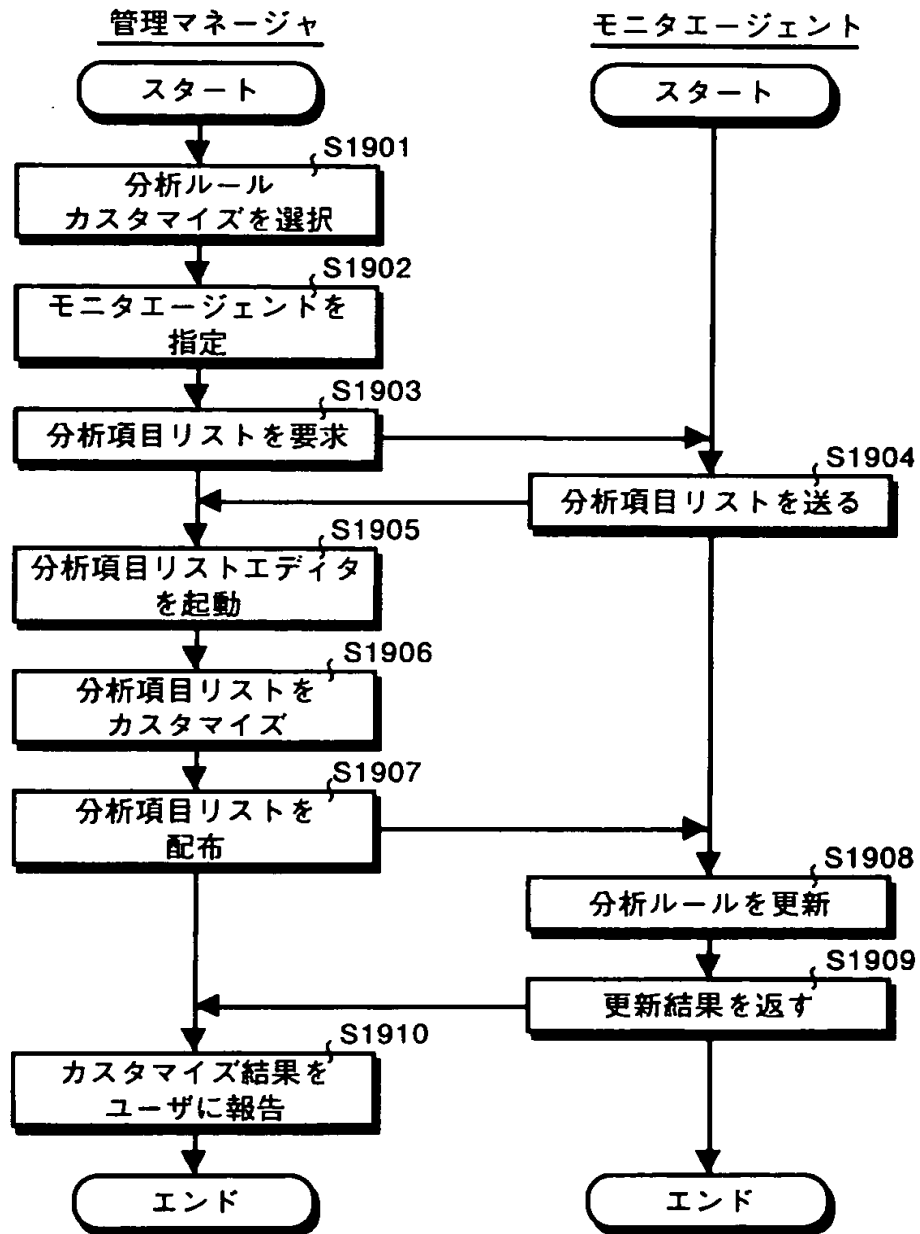
【図 18】

分析ルールを更新する際の管理マネージャとモニタエージェントの処理手順を示すフローチャート



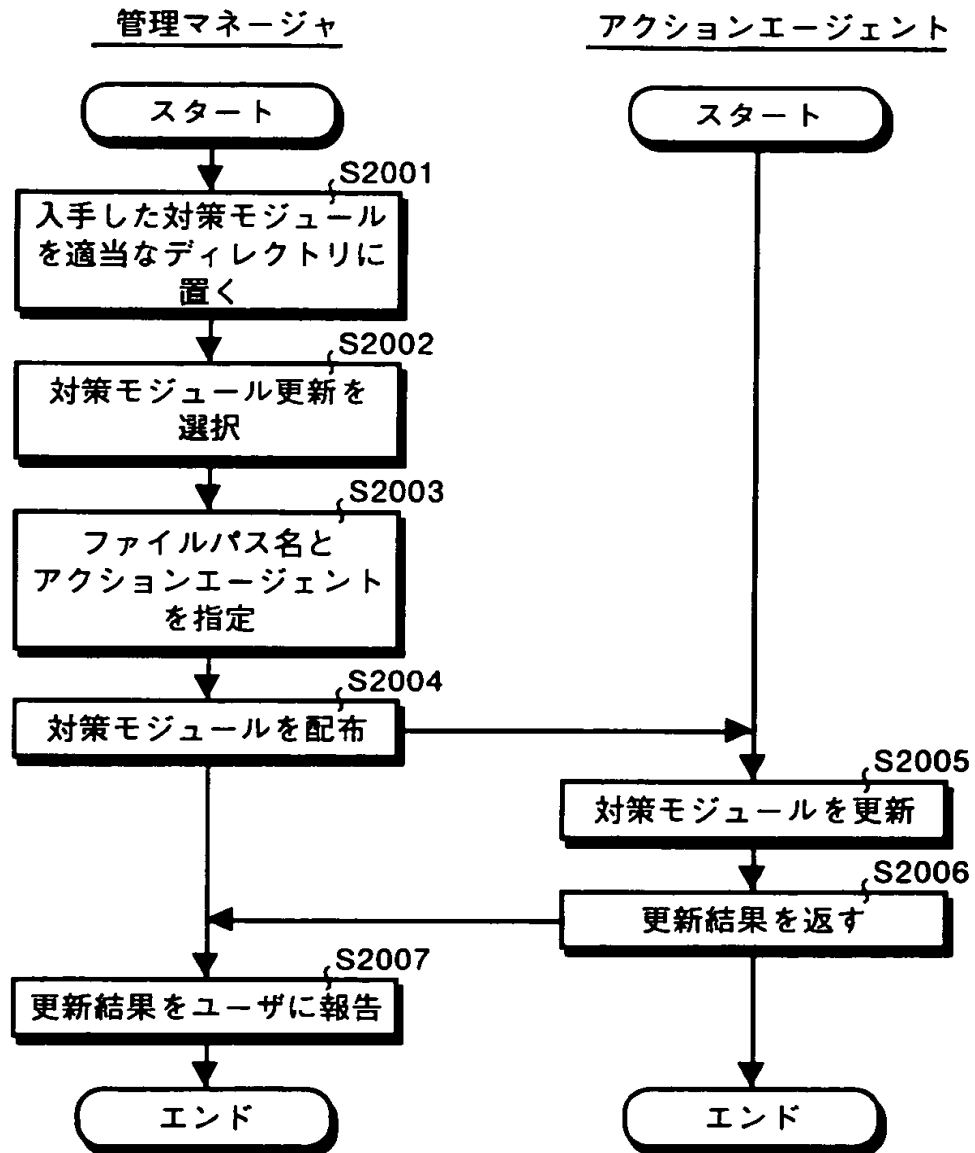
【図19】

分析ルールをカスタマイズする際の管理マネージャとモニタエージェントの
処理手順を示すフローチャート



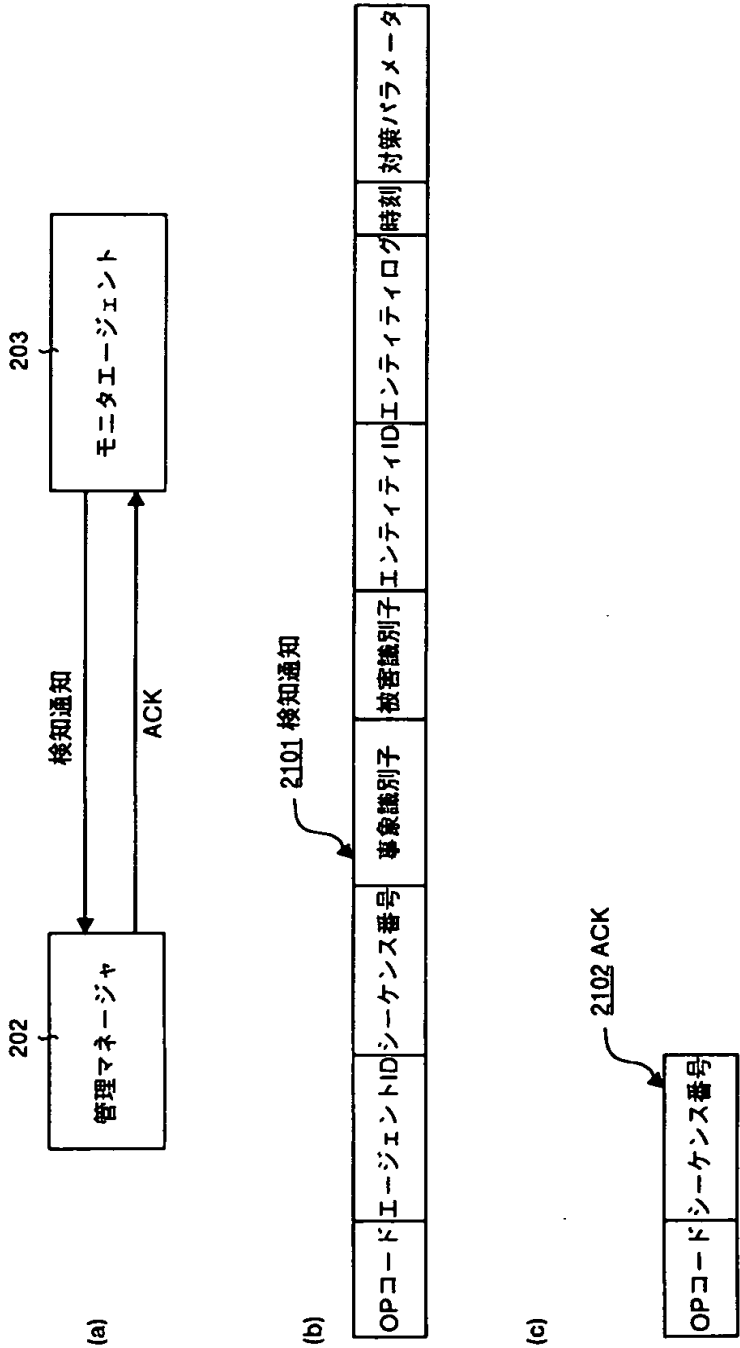
【図20】

対策モジュールの更新手順を示すフローチャート



【図 2 1】

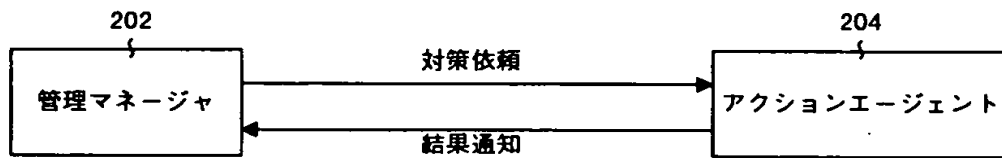
管理マネージャとモニタエージェントとの間で授受される検知通知
およびACKのデータ構造の一例を示す図



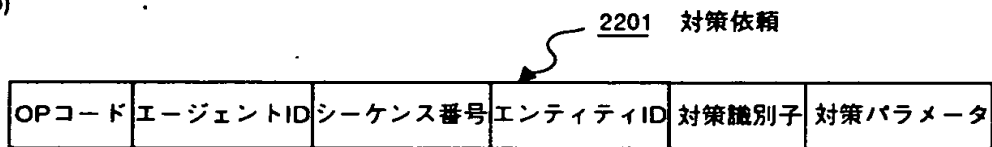
【図 2 2】

管理マネージャとアクションエージェントとの間で授受される対策依頼
および結果通知のデータ構造の一例を示す図

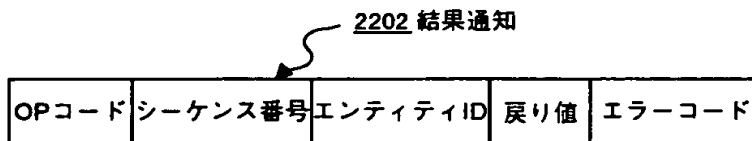
(a)



(b)

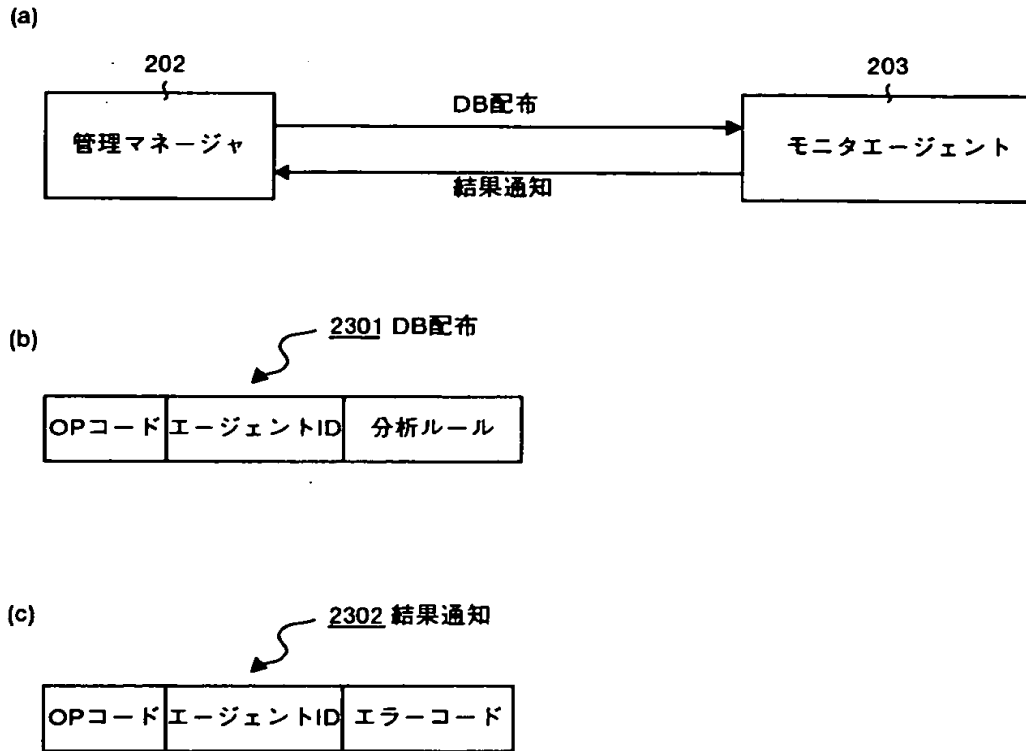


(c)



【図 2 3】

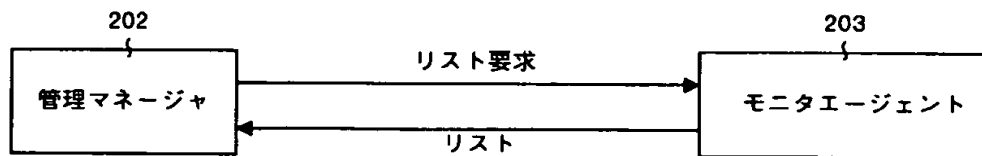
管理マネージャとモニタエージェントとの間で授受されるDB（分析ルール）配布
および結果通知のデータ構造の一例を示す図



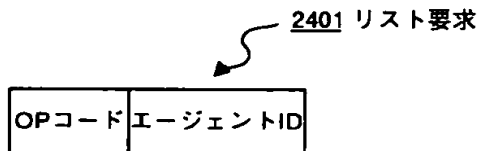
【図 2 4】

管理マネージャとモニタエージェントとの間で授受されるリスト要求
およびリストのデータ構造の一例を示す図

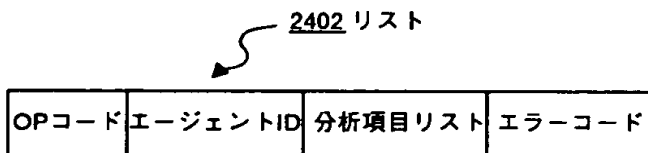
(a)



(b)

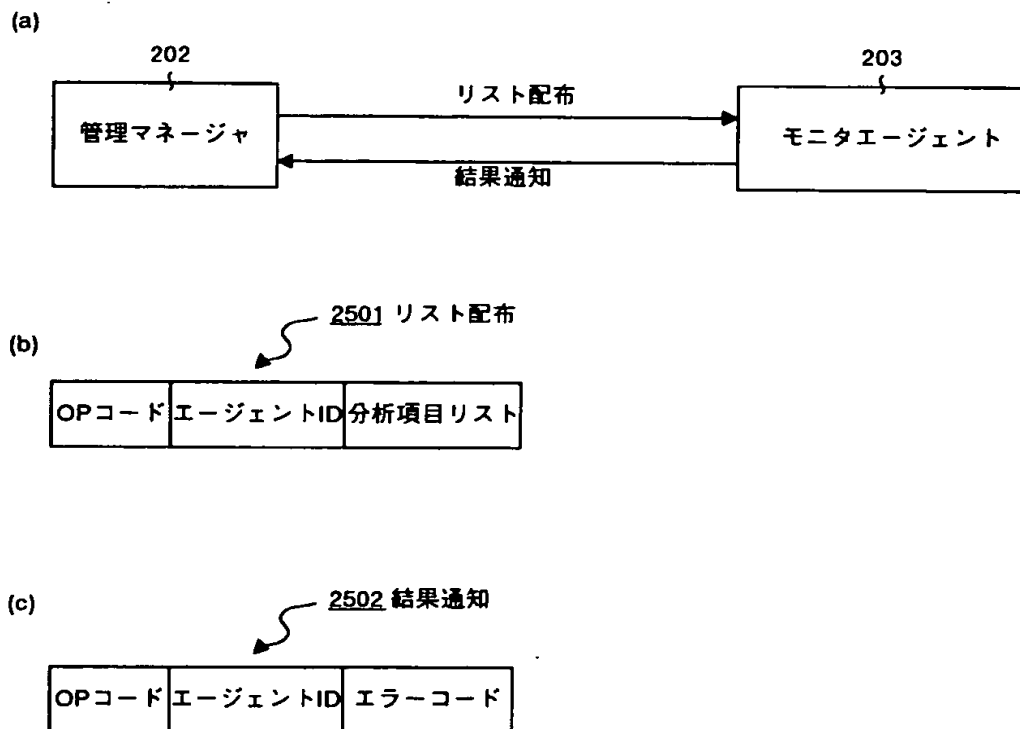


(c)



【図 2 5】

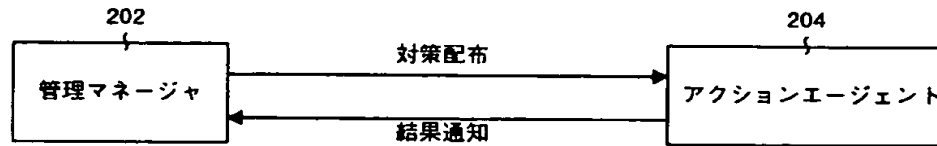
管理マネージャとモニタエージェントとの間で授受されるリスト配布
および結果通知のデータ構造の一例を示す図



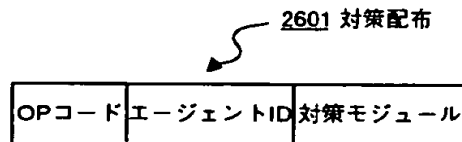
【図 2 6】

管理マネージャとアクションエージェントとの間で授受される対策配布
および結果通知のデータ構造の一例を示す図

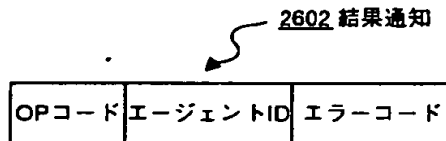
(a)



(b)

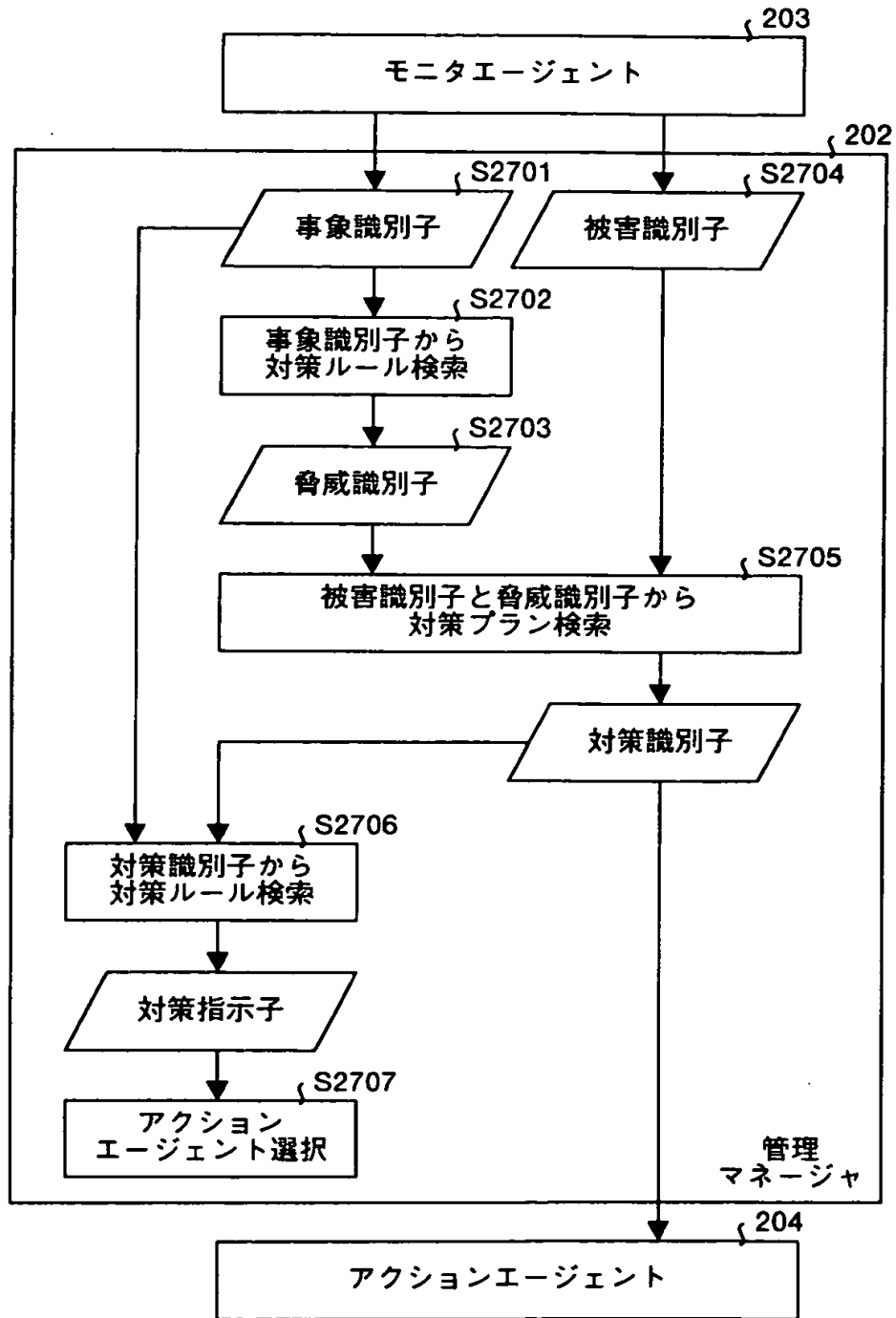


(c)



【図 27】

管理マネージャがおこなう対策決定処理を説明するための説明図



【図 2 8】

対策プランの一例を示す図

(a)	事象識別子	被害識別子
	事象001	被害あり

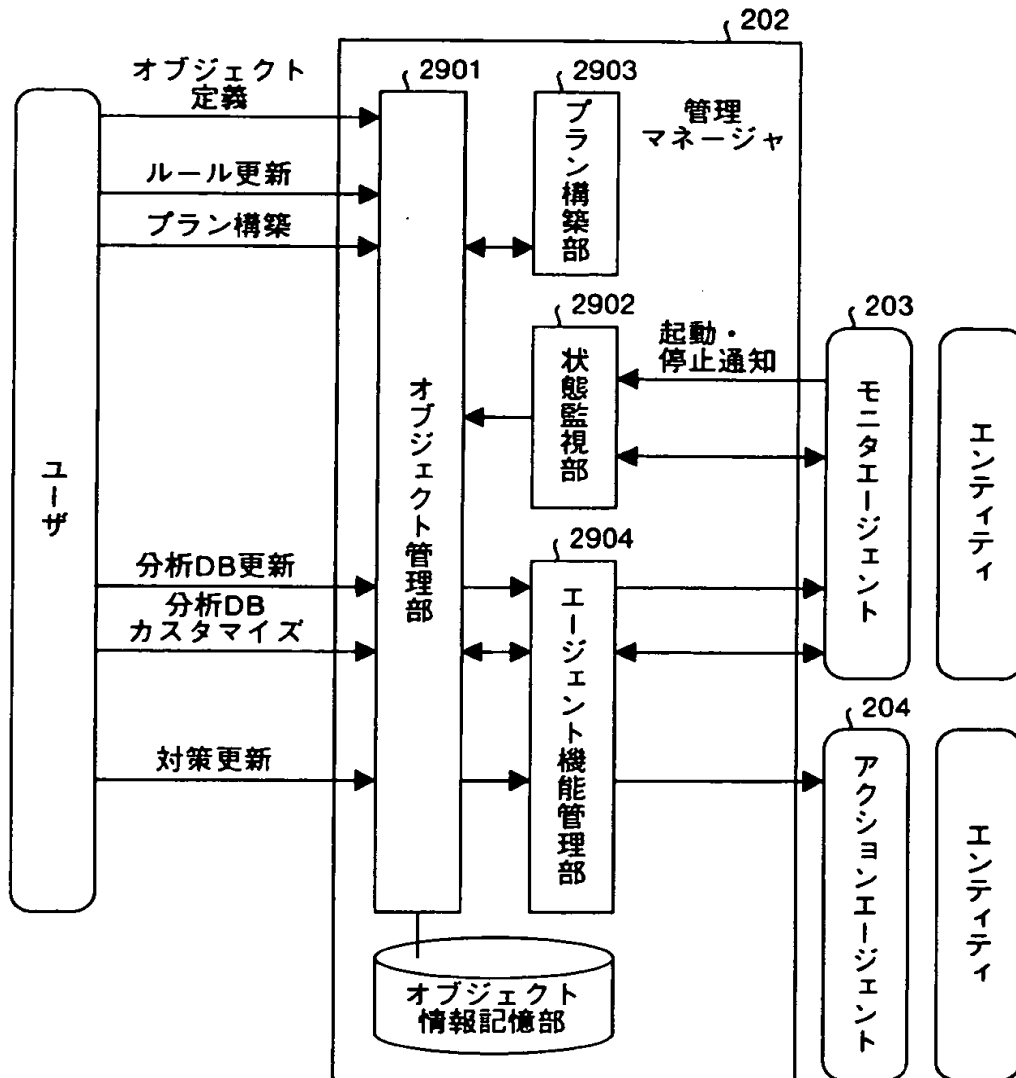
(b)	対策ルール			
	事象識別子	脅威識別子	対策識別子	対策指示子
	事象001	脅威001	対策001	SERVER
	事象001	脅威001	対策002	FW
	事象002	脅威001	対策001	SERVER
	事象002	脅威001	対策002	FW
	事象003	脅威010	対策011	SERVER
	事象003	脅威010	対策012	SERVER
	事象003	脅威010	対策012	FW

(c)	対策プラン		
	事象識別子	脅威識別子	対策識別子
	被害あり	脅威001	対策001
	被害不明	脅威001	対策002
	被害なし	脅威001	—
	被害あり	脅威002	対策011
	被害不明	脅威002	—
	被害なし	脅威002	—

(d)	対策ルール			
	事象識別子	脅威識別子	対策識別子	対策指示子
	事象001	脅威001	対策001	SERVER
	事象001	脅威001	対策002	FW
	事象002	脅威001	対策001	SERVER
	事象002	脅威001	対策002	FW
	事象003	脅威010	対策011	SERVER
	事象003	脅威010	対策012	SERVER
	事象003	脅威010	対策012	FW

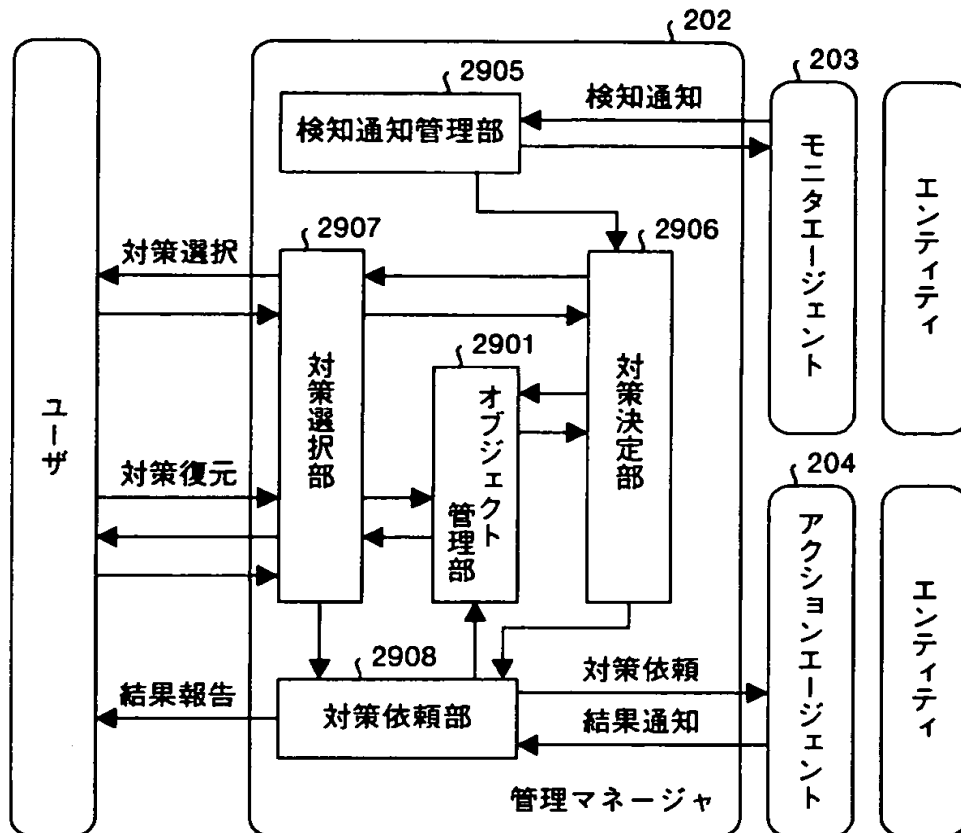
【図 29】

管理マネージャの機能的な構成を示すブロック図



【図 3 0】

管理マネージャの機能的な構成を示すブロック図



【図 3 1】

管理マネージャオブジェクトを示す図

属性		説明
管理 マネージャ	ID	オブジェクト定義時に、 管理マネージャが割り当てる
	IPアドレス	エージェントから管理マネージャへの 通信に必要なとなる情報。 ポート番号は、モニタエージェント 用、アクションエージェント用の2つ
	ポート番号 (1)	
	ポート番号 (2)	
	通信タイムアウト値	
	通信リトライ回数	
対策ルール	ファイル名 (複数可)	対策ルールファイルへのパスを 指定する
対策プラン	ファイル名	対策プランファイルへのパスを 指定する
ログフォー マット定義	ファイル名	管理マネージャは、モニタエージェン トから送られるエンティティログから 時間を引き出す
エージェント 認定リスト	ファイル名	認定機関によって認定されたエージェ ントのリスト。管理マネージャは、リ ストにないエージェントからの処理を 受け付けない
状態監視	時間間隔	エージェントの状態を確認する間隔を 指定する
モニタ エージェント	ID (複数可)	モニタエージェントをオブジェクト定 義すると、自動的に追加される
アクション エージェント	ID (複数可)	アクションエージェントをオブジェク ト定義すると、自動的に追加される

【図 3 2】

エージェントオブジェクトを示す図

属性		説明
エージェント	ID	オブジェクト定義に、管理マネージャが割り当てる
	ステータス	動作状態を示す
	IPアドレス	管理マネージャからエージェントへの通信に必要な情報
	ポート番号	
	通信タイムアウト値	
	通信リトライ回数	
エンティティ	ID	エージェントの対象エンティティ
管理マネージャ	ID	エージェントの管理マネージャ

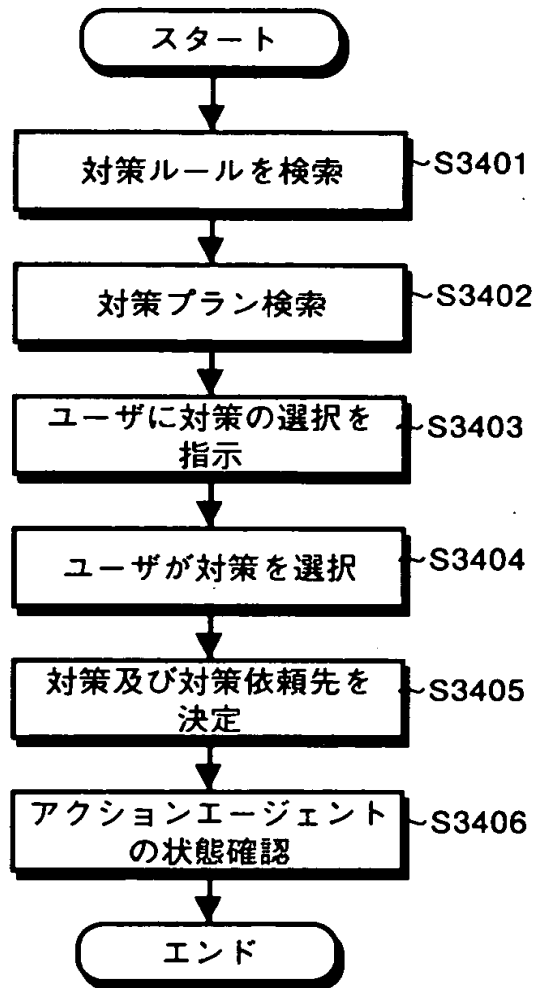
【図 3 3】

エンティティオブジェクトを示す図

属性		説明
エンティティ	ID	オブジェクト定義時に、管理マネージャが割り当てる
	IPアドレス	エージェントからエンティティへの通信に必要な情報
	ポート番号	
	通信タイムアウト値	
	通信リトライ回数	
FWエンティティ	ID	エンティティのファイアウォールにあたるエンティティ
モニタエージェント	ID	モニタエージェントをオブジェクト定義すると、自動的に追加される
アクションエージェント	ID	アクションエージェントをオブジェクト定義すると、自動的に追加される
対策履歴	(複数可)	対策依頼、もしくは対策結果を履歴として残す
エンティティ固有情報	FireWall-1	FireWall-1オブジェクト名

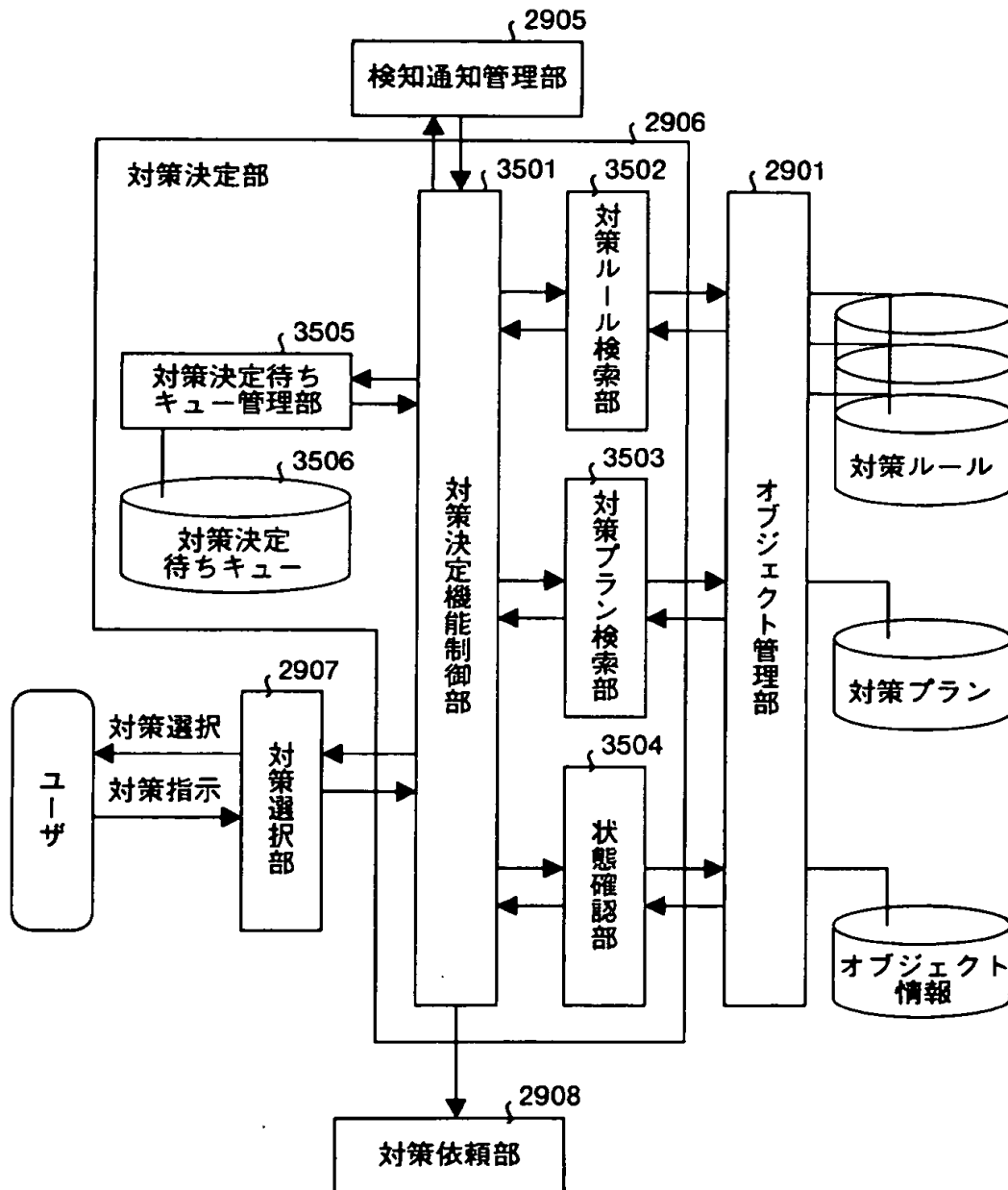
【図 3 4】

対策決定部による対策決定までの処理手順を示すフローチャート



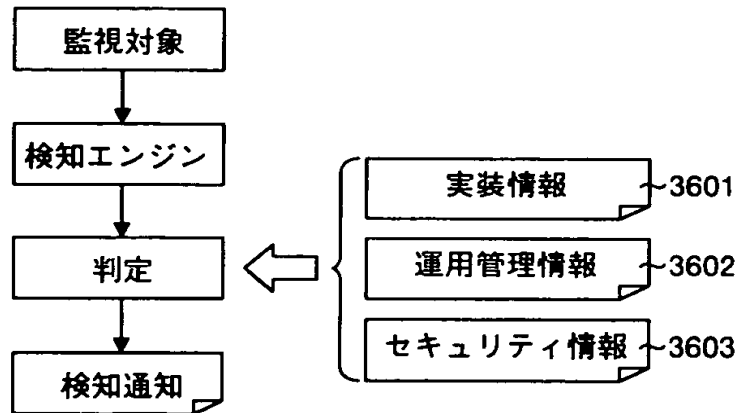
【図 35】

対策決定部の構成を示す機能ブロック図



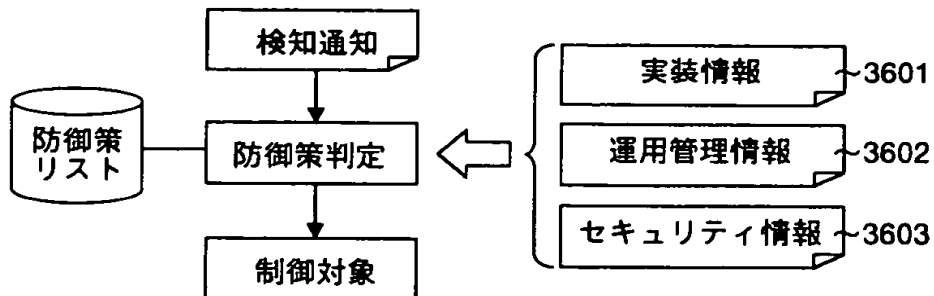
【図 36】

レポート機能の説明するための説明図



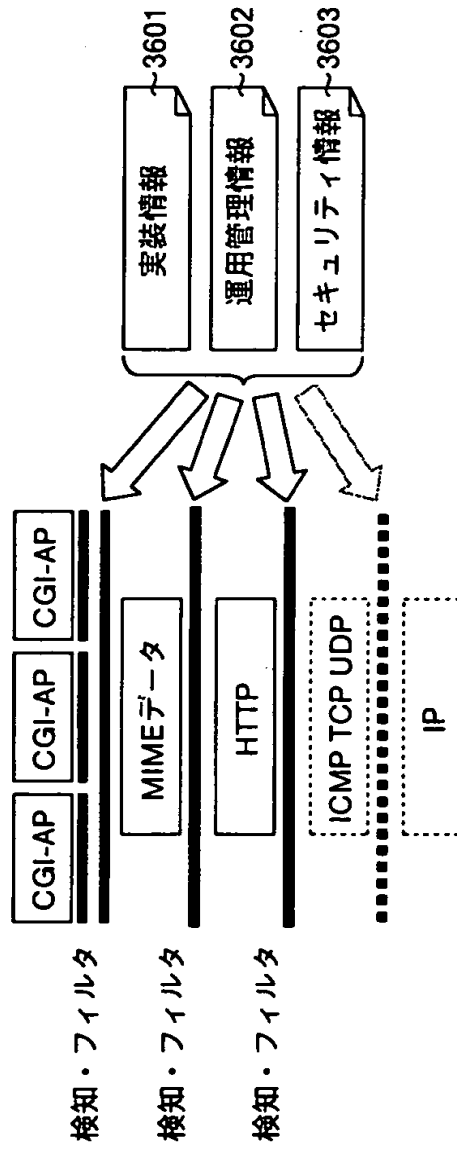
【図 37】

実装情報などを用いた多面的な防御策選択を説明するための説明図



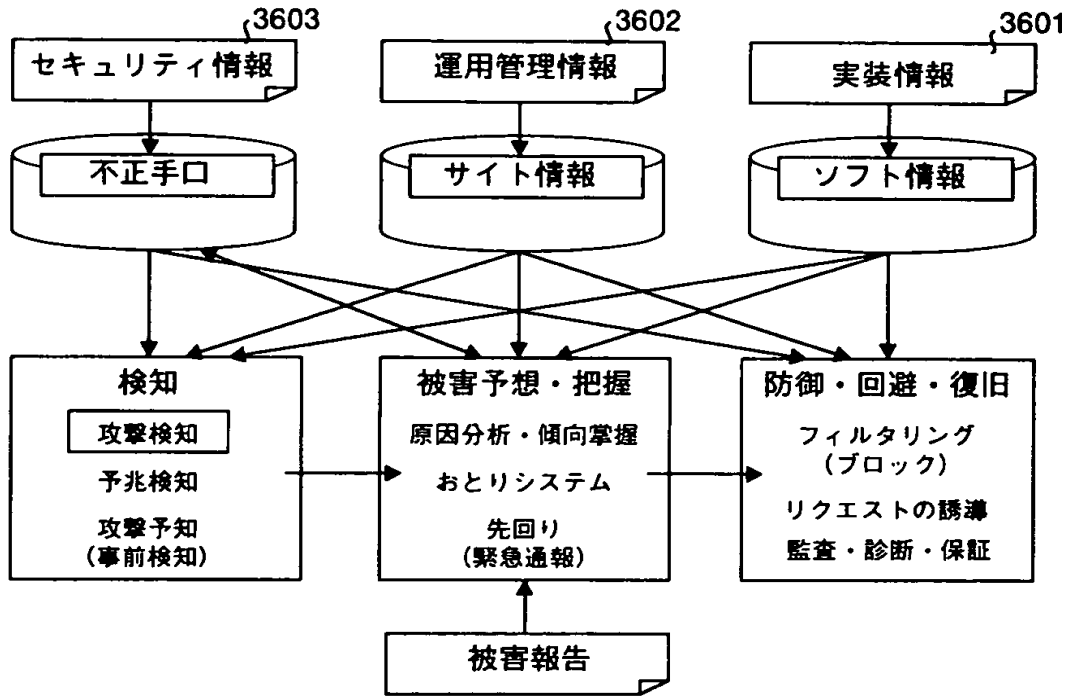
【図 38】

実装情報などをプロトコル階層間のフィルタとして用いる概念を
説明するための説明図



【図 39】

実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図



【書類名】 要約書

【要約】

【課題】 サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることを課題とする。

【解決手段】 モニタエージェント 2 0 3 でエンティティのログを分析し、異常の予兆を検知した場合には、管理マネージャ 2 0 2 に通知する。そして、この管理マネージャ 2 0 2 は、データベース 2 0 1 などに基づいて対策および対策依頼先を決定し、対策依頼先であるアクションエージェント 2 0 4 に該当する対策を実施させる。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.